AVG Internet Security 2013

Manuale per l'utente

Revisione documento 2013.01 (30.8.2012)

Sommario

1. Introduzione

Questa guida per l'utente fornisce la documentazione completa relativa a **AVG Internet Security 2013**.

Grazie ai diversi livelli di protezione per tutte le attività svolte in linea offerti da **AVG Internet Security 2013**, il furto d'identità, i virus o i siti pericolosi non sono più un problema. Con le funzionalità Tecnologia di protezione cloud AVG e Rete di protezione della community AVG incluse nel prodotto, le informazioni sulle minacce più recenti vengono raccolte e condivise con la community per fornire una protezione ottimale. È possibile effettuare acquisti e usufruire dei servizi di banking in linea in modo sicuro, utilizzare i social network o esplorare ed eseguire ricerche in tutta sicurezza con la protezione in tempo reale.

2. Requisiti per l'installazione di AVG

2.1. Sistemi operativi supportati

AVG Internet Security 2013 è destinato alla protezione delle workstation che eseguono i seguenti sistemi operativi:

- Windows XP Home Edition SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista (x86 e x64, tutte le edizioni)
- Windows 7 (x86 e x64, tutte le edizioni)

(ed eventualmente Service Pack successivi per sistemi operativi specifici)

Nota*: il componente Identity non è supportato in Windows XP x64. Su questo sistema operativo è possibile installare AVG Internet Security 2013, ma solo senza il componente IDP.*

2.2. Requisiti hardware minimi e consigliati

Requisiti hardware minimi per **AVG Internet Security 2013**:

- CPU Intel Pentium da 1.5 GHz o superiore
- 512 MB (Windows XP) / 1024 MB (Windows Vista, Windows 7) di memoria RAM
- 1,3 GB di spazio libero sul disco rigido *(per scopi di installazione)*

Requisiti hardware consigliati per **AVG Internet Security 2013**:

- CPU Intel Pentium da 1.8 GHz o superiore
- 1024 MB di memoria RAM
- 1,6 GB di spazio libero sul disco rigido *(per scopi di installazione)*

3. Processo di installazione di AVG

Dove posso trovare il file di installazione?

Per installare **AVG Internet Security 2013** nel computer è necessario disporre del file di installazione più recente. Per assicurarsi di installare la versione aggiornata di **AVG Internet Security 2013**, si consiglia di scaricare il file di installazione dal sito Web di AVG (http://www.avg.com/). La sezione ***Centro di assistenza / Download*** fornisce una panoramica strutturata dei file di installazione per ciascuna edizione di AVG.

In caso di dubbi sui file da scaricare e installare, è possibile utilizzare il servizio ***Seleziona prodotto*** disponibile nella parte inferiore della pagina Web. Tramite le risposte a tre semplici domande il servizio definisce i file necessari. Fare clic sul pulsante ***Procedi*** per visualizzare l'elenco completo dei file per il download personalizzati in base alle esigenze specifiche.

Com'è strutturato il processo di installazione?

Dopo aver scaricato e salvato il file di installazione sul disco rigido, è possibile avviare il processo di installazione. L'installazione è una sequenza di finestre di dialogo semplici e chiare. Ciascuna finestra di dialogo descrive brevemente come procedere in ciascuna fase del processo di installazione. Di seguito viene fornita una descrizione dettagliata di ciascuna finestra di dialogo:

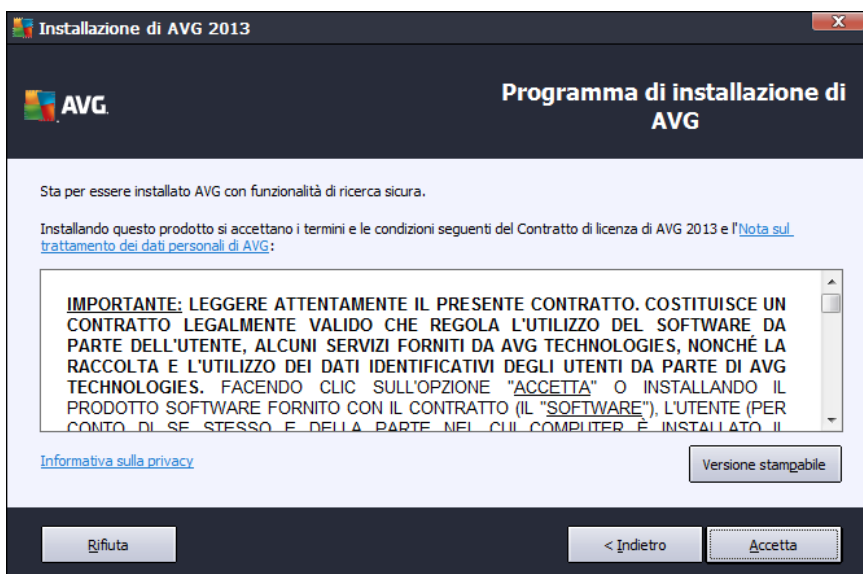
3.1. Finestra introduttiva: selezione della lingua

Il processo di installazione comincia con la finestra di dialogo ***Benvenuti nel programma di installazione di AVG***:

In questa finestra di dialogo è possibile selezionare la lingua utilizzata per il processo di installazione. Fare clic sulla casella combinata per visualizzare il menu a discesa della lingua. Selezionare la lingua desiderata. Il processo di installazione procederà quindi nella lingua prescelta.

Attenzione: in questa fase viene selezionata solo la lingua per il processo di installazione. L'applicazione AVG Internet Security 2013 verrà installata nella lingua selezionata e in inglese, lingua sempre installata automaticamente. Tuttavia, è possibile installare più lingue e utilizzare AVG Internet Security 2013 in qualsiasi di queste lingue. Verrà richiesto di confermare la selezione di lingue alternative in una delle seguenti finestre di dialogo di installazione denominata Opzioni personalizzate.

3.2. Finestra introduttiva: contratto di licenza

Inoltre, la finestra di dialogo ***Benvenuti nel programma di installazione di AVG*** fornisce il testo completo del Contratto di licenza AVG:

Leggere con attenzione l'intero testo. Leggere con attenzione il contratto e confermarne lettura e accettazione selezionando il pulsante ***Accetto***. Se non si accettano i termini del contratto di licenza, fare clic sul pulsante ***Rifiuta***. Il processo di installazione verrà interrotto immediatamente.

Informativa sulla privacy di AVG

Oltre al Contratto di licenza, questa finestra di dialogo di installazione offre ulteriori informazioni circa l'***Avviso sulla tutela dei dati personali di AVG*** e l'***Informativa sulla privacy di AVG*** *(tutte le suddette funzioni vengono visualizzate nella finestra di dialogo sotto forma di un collegamento ipertestuale attivo che consente di accedere al sito Web dedicato in cui si trovano le informazioni dettagliate)*. Fare clic sul relativo collegamento per essere reindirizzati al sito Web di AVG (http://www.avg.com/) in cui è possibile trovare il testo completo di tali informative.

Pulsanti di controllo

Nella prima finestra di dialogo di installazione, sono disponibili solo due pulsanti di controllo:

- ***Versione stampabile***: fare clic sul pulsante per visualizzare il testo completo del Contratto di licenza di AVG in un'interfaccia Web e strutturato chiaramente per la stampa.

- ***Rifiuta***: fare clic per rifiutare il Contratto di licenza. Il processo di installazione verrà chiuso immediatamente. **AVG Internet Security 2013** non verrà installato.
- ***Indietro***: fare clic per tornare alla precedente finestra di dialogo di installazione.
- ***Accetta***: fare clic per confermare che il Contratto di licenza è stato letto e accettato. L'installazione continuerà con la successiva finestra di dialogo.

3.3. Attiva la licenza di AVG

Nella finestra di dialogo ***Attiva la licenza*** viene richiesto di immettere il License Number nel campo di testo fornito:

Dove è possibile reperire il License Number

Il Sales Number è disponibile sulla custodia del CD presente nella confezione di **AVG Internet Security 2013**. Il License Number sarà contenuto nel messaggio e-mail di conferma ricevuto dopo l'acquisto in linea di **AVG Internet Security 2013**. È necessario digitare il numero esattamente come viene indicato. Se il License Number è disponibile nel formato digitale (*contenuto nel messaggio e-mail*), si consiglia di utilizzare il metodo "copia e incolla" per immetterlo.

Come utilizzare il metodo Copia e incolla

L'uso del metodo ***Copia e incolla*** per immettere il License Number di **AVG Internet Security 2013** nel programma assicura un'immissione corretta. Procedere come segue:

- Aprire il messaggio e-mail che contiene il License Number.
- Posizionare il cursore all'inizio del License Number, premere il pulsante sinistro del mouse e, mantenendolo premuto, fare scorrere il cursore sul numero di licenza, quindi rilasciare il pulsante. Il numero viene evidenziato.

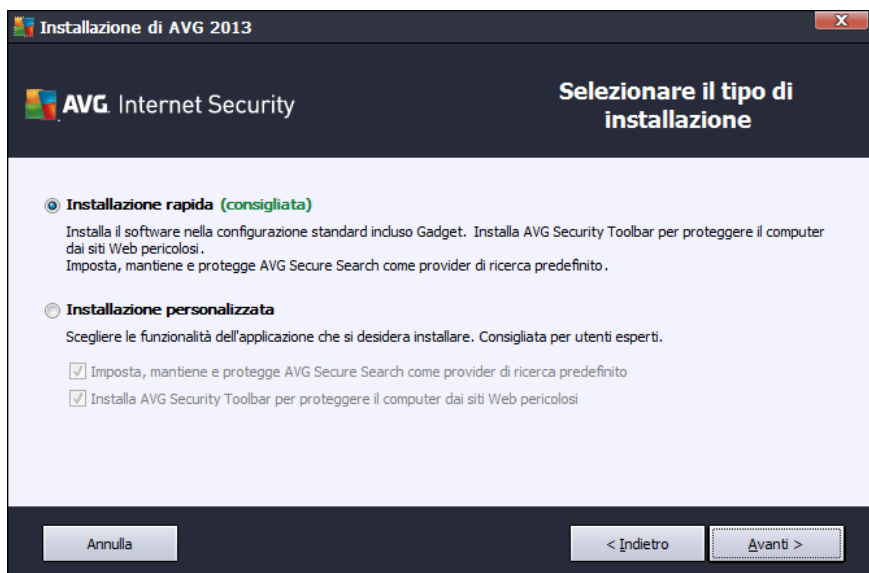
- Tenere premuto ***Ctrl***, quindi premere ***C***. Questa operazione copia il numero.
- Fare clic nella posizione in cui si desidera incollare il numero copiato.
- Tenere premuto ***Ctrl***, quindi premere ***V***. Questa operazione incolla il numero nella posizione selezionata.

Pulsanti di controllo

Come avviene per la maggior parte delle finestre di dialogo, sono disponibili tre pulsanti di controllo:

- ***Annulla***: fare clic per uscire subito dal processo di installazione. **AVG Internet Security 2013** non verrà installato.
- ***Indietro***: fare clic per tornare alla precedente finestra di dialogo di installazione.
- ***Avanti***: fare clic per procedere con la successiva finestra di dialogo di installazione.

3.4. Selezionare il tipo di installazione

La finestra di dialogo ***Selezionare il tipo di installazione*** offre due opzioni di installazione: ***Installazione rapida*** e ***Installazione personalizzata***:

Installazione rapida

Per la maggior parte degli utenti è consigliabile mantenere l'installazione ***rapida*** standard. In questo modo, **AVG Internet Security 2013** viene installato in modalità completamente automatica con le impostazioni predefinite dal produttore del software, inclusi gadget AVG, AVG Security Toolbar e AVG Secure Search configurato come provider di ricerca predefinito. Questa configurazione fornisce la massima protezione combinata con l'utilizzo ottimale delle risorse. In futuro, se ci fosse necessità

di modificare la configurazione, sarà possibile farlo direttamente nell'applicazione **AVG Internet Security 2013**.

Premere il pulsante ***Avanti*** per passare alla finestra di dialogo successiva del processo di installazione:

Installazione personalizzata

L'***installazione personalizzata*** deve essere utilizzata solo da utenti esperti che hanno valide ragioni per installare **AVG Internet Security 2013** con impostazioni non standard, ad esempio per soddisfare specifici requisiti di sistema. In questa sezione è possibile decidere se installare le seguenti funzionalità *(entrambe le funzionalità sono contrassegnate per l'installazione e verranno installate automaticamente a meno che non le si deselezioni)*:

- ***Imposta, mantiene e protegge AVG Secure Search come provider di ricerca predefinito***: lasciare selezionata l'opzione per confermare che si desidera utilizzare il motore AVG Secure Search, che funziona insieme al componente LinkScanner Surf-Shield per assicurare la massima protezione in linea.

- ***Installa AVG Security Toolbar per proteggere il computer dai siti Web pericolosi***: lasciare selezionata l'opzione per installare AVG Security Toolbar e assicurare la massima protezione durante l'esplorazione di Internet.

Se si decide di utilizzare questa opzione, una nuova sezione chiamata ***Cartella di destinazione*** verrà visualizzata nella finestra di dialogo. Qui è possibile specificare il percorso in cui **AVG Internet Security 2013** deve essere installato. Per impostazione predefinita, **AVG Internet Security 2013** verrà installato nella cartella Programmi nell'unità C:, come indicato nel campo di testo della finestra di dialogo. Se si desidera modificare questo percorso, utilizzare il pulsante ***Sfoglia*** per visualizzare la struttura dell'unità e selezionare la cartella appropriata. Per ripristinare la destinazione predefinita dal fornitore del software, utilizzare il pulsante ***Predefinita***.

Premere quindi il pulsante ***Avanti*** per passare alla finestra di dialogo Opzioni personalizzate.

Pulsanti di controllo

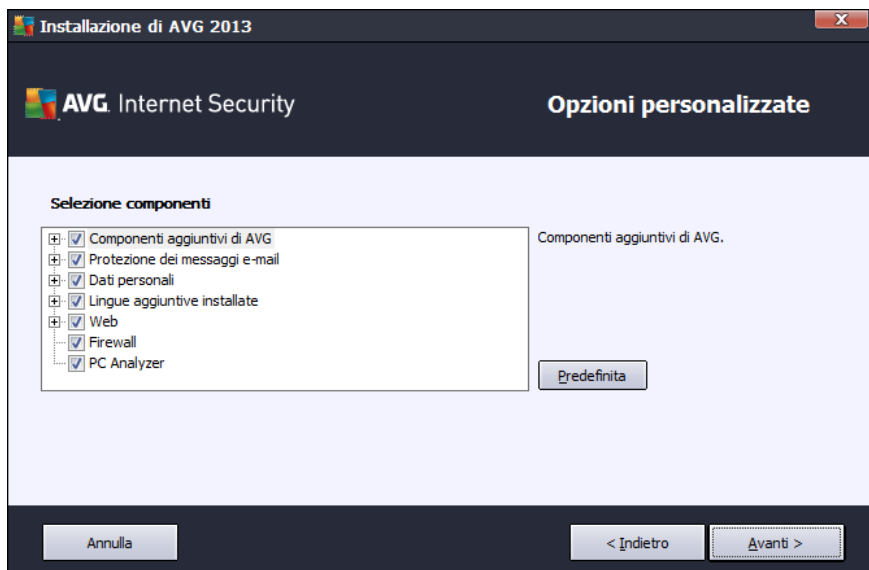
Come avviene per la maggior parte delle finestre di dialogo di impostazione, sono disponibili tre pulsanti di controllo:

- ***Annulla***: fare clic per uscire subito dal processo di installazione. **AVG Internet Security 2013** non verrà installato.

- ***Indietro***: fare clic per tornare alla precedente finestra di dialogo di installazione.

- ***Avanti***: fare clic per procedere con la successiva finestra di dialogo di installazione.

3.5. Opzioni personalizzate

La finestra di dialogo ***Opzioni personalizzate*** consente di impostare parametri di installazione dettagliati:

La sezione ***Selezione componenti*** visualizza una panoramica di tutti i componenti di **AVG Internet Security 2013** che è possibile installare. Se le impostazioni predefinite non sono adeguate alle esigenze specifiche, è possibile rimuovere/aggiungere determinati componenti.

È tuttavia possibile eseguire la selezione solo tra i componenti inclusi nell'edizione di AVG che è stata acquistata.

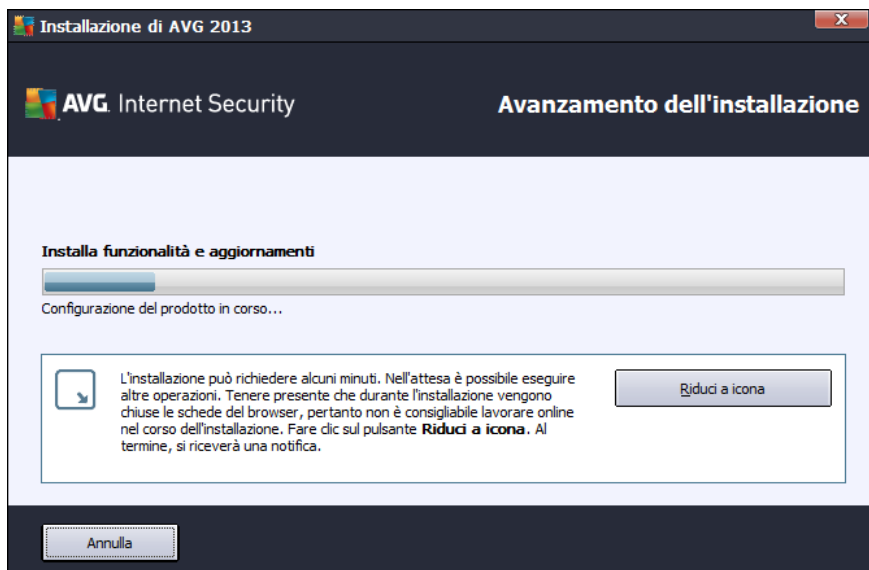
Evidenziare una voce dell'elenco ***Selezione componenti*** per visualizzare una breve descrizione del relativo componente nella parte destra della sezione. Per informazioni dettagliate sulla funzionalità di ciascun componente, consultare il capitolo Panoramica dei componenti di questo documento. Per ripristinare la configurazione predefinita dal fornitore del software, utilizzare il pulsante ***Predefinita***.

Pulsanti di controllo

Come avviene per la maggior parte delle finestre di dialogo, sono disponibili tre pulsanti di controllo:

- ***Annulla***: fare clic per uscire subito dal processo di installazione. **AVG Internet Security 2013** non verrà installato.
- ***Indietro***: fare clic per tornare alla precedente finestra di dialogo di installazione.
- ***Avanti***: fare clic per procedere con la successiva finestra di dialogo di installazione.

3.6. Avanzamento dell'installazione

Nella finestra di dialogo ***Avanzamento dell'installazione*** viene visualizzato l'avanzamento del processo di installazione. Non è necessario alcun intervento da parte dell'utente:

Al termine dell'installazione, si verrà reindirizzati automaticamente alla seguente finestra di dialogo.

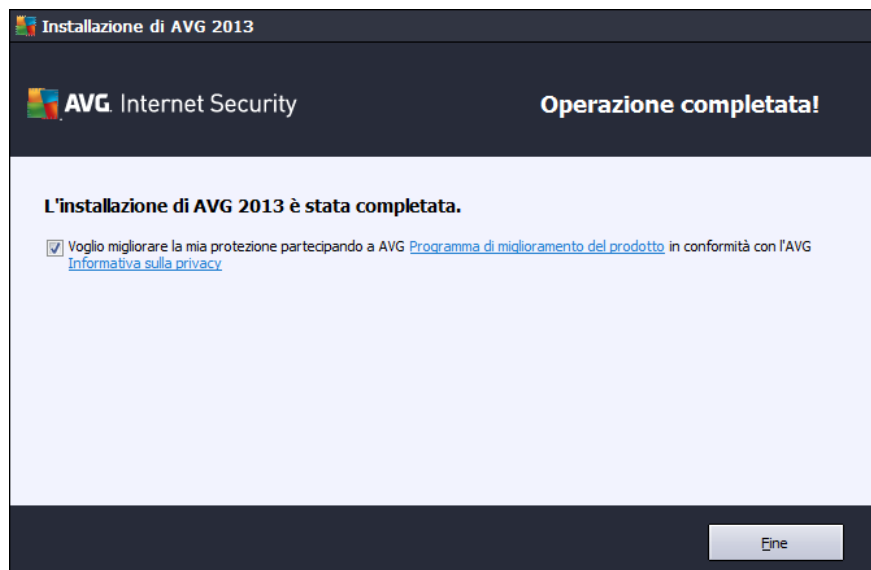
Pulsanti di controllo

In questa finestra di dialogo sono disponibili due pulsanti di controllo:

- ***Riduci a icona***: il processo di installazione potrebbe richiedere alcuni minuti. Fare clic sul pulsante per ridurre a icona la finestra di dialogo in un'icona visibile nella barra di sistema. La finestra di dialogo viene nuovamente visualizzata dopo aver completato l'installazione.

- ***Annulla***: questo pulsante deve essere utilizzato solo se si desidera arrestare il processo di installazione in corso. In tal caso **AVG Internet Security 2013** non verrà installato.

3.7. Installazione completata

La finestra di dialogo ***Installazione completata*** conferma che **AVG Internet Security 2013** è stato installato e configurato correttamente:

Programma di miglioramento del prodotto di AVG e Informativa sulla privacy di AVG

Permette di decidere se partecipare al ***Programma di miglioramento del prodotto*** (*per dettagli, vedere il capitolo Impostazioni avanzate di AVG / Programma di miglioramento del prodotto*) che raccoglie informazioni anonime sulle minacce rilevate per aumentare il livello globale di protezione in Internet. Tutti i dati sono considerati riservati e in conformità all'Informativa sulla privacy di AVG. Fare clic sul collegamento ***Informativa sulla privacy*** per essere reindirizzati al sito Web di AVG (http://www.avg.com/) in cui è possibile trovare il testo completo dell'Informativa sulla privacy di AVG. Se si accetta, mantenere l'opzione selezionata *(l'opzione viene confermata per impostazione predefinita)*.

Riavvio del computer

Per completare il processo di installazione è necessario riavviare il computer: selezionare ***Riavvia subito*** per riavviare il computer immediatamente oppure ***Riavvia in seguito*** per posticipare l'operazione.

4. Dopo l'installazione

4.1. Registrazione del prodotto

Al termine dell'installazione di **AVG Internet Security 2013**, registrare il prodotto in linea nel sito Web di AVG *(http://www.avg.com/)*. Dopo la registrazione sarà possibile ottenere l'accesso completo all'account utente AVG, alla newsletter di aggiornamento AVG e ad altri servizi offerti esclusivamente agli utenti registrati. Il modo più facile per effettuare la registrazione è quello di procedere direttamente dall'interfaccia utente di **AVG Internet Security 2013**. Nel menu di spostamento superiore, selezionare la voce Opzioni / Registra ora. Si verrà reindirizzati alla pagina della ***registrazione*** del sito Web di AVG *(http://www.avg.com/)*. Seguire le istruzioni fornite nella pagina.

4.2. Accesso all'interfaccia utente

È possibile accedere alla finestra di dialogo principale di AVG in diversi modi:

- tramite doppio clic sull'icona di AVG sulla barra delle applicazioni
- tramite doppio clic sull'icona di AVG sul desktop
- dal menu ***Start / Tutti i programmi / AVG / AVG 2013***

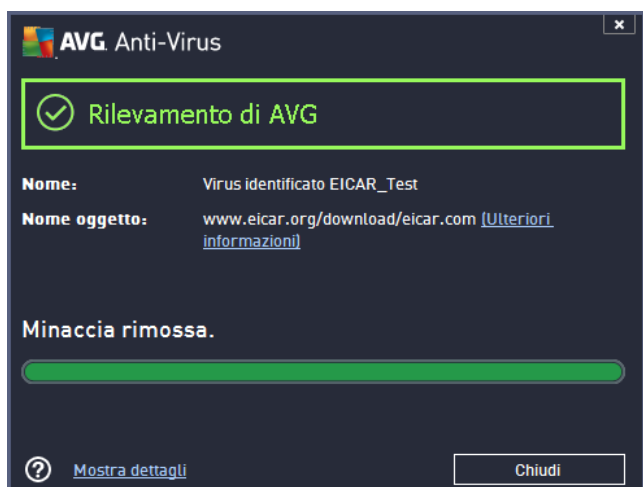
4.3. Scansione dell'intero computer

Esiste il rischio potenziale che un virus sia stato trasmesso al computer dell'utente prima dell'installazione di **AVG Internet Security 2013**. Per questo motivo è necessario eseguire Scansione intero computer per assicurarsi che non siano presenti infezioni sul PC. La prima scansione potrebbe richiedere diverso tempo *(circa un'ora)*, ma si consiglia di eseguirla comunque per verificare che il computer non sia stato compromesso da una minaccia. Per istruzioni sull'esecuzione di Scansione intero computer, consultare il capitolo Scansione AVG.

4.4. Controllo Eicar

Per confermare che **AVG Internet Security 2013** è stato installato correttamente è possibile eseguire il controllo EICAR.

Il controllo EICAR è un metodo standard e assolutamente sicuro per verificare il funzionamento del sistema antivirus. La sua esecuzione è sicura poiché non si tratta di un vero virus e non include frammenti di codice virale. La maggior parte dei prodotti vi reagisce come se si trattasse di un virus, *anche se normalmente lo segnala con un nome ovvio come "EICAR-AV-Test"*. È possibile scaricare il virus EICAR dal sito Web di EICAR all'indirizzo www.eicar.com, in cui si troveranno anche tutte le informazioni necessarie sul controllo EICAR.

Provare a scaricare il file *eicar.com* e a salvarlo sul disco locale. Subito dopo aver confermato il download del file di controllo, **AVG Internet Security 2013** visualizzerà un avviso. Questo avviso dimostra che AVG è stato installato correttamente nel computer.

Se AVG non identifica il file di controllo EICAR come un virus, è necessario verificare nuovamente la configurazione del programma.

4.5. Configurazione predefinita di AVG

La configurazione predefinita (*ovvero la modalità di impostazione dell'applicazione dopo l'installazione*) di **AVG Internet Security 2013** è impostata dal fornitore del software in modo tale che tutti i componenti e le funzioni offrano un'ottimizzazione massima delle prestazioni.

A meno che non vi sia un motivo valido, si consiglia di non modificare la configurazione di AVG. Le eventuali modifiche alle impostazioni devono essere eseguite solo da utenti esperti.

È possibile apportare alcune modifiche minori alle impostazioni dei componenti di AVG direttamente dall'interfaccia utente del componente specifico. Se si desidera modificare la configurazione di AVG per adeguare l'applicazione alle proprie esigenze, accedere a Impostazioni AVG avanzate: selezionare la voce del *menu principale Impostazioni avanzate* e modificare la configurazione di AVG nella finestra di dialogo Impostazioni AVG avanzate visualizzata.

5. Interfaccia utente di AVG

AVG Internet Security 2013 si apre visualizzando la finestra principale:

La finestra principale è suddivisa in diverse sezioni:

- ***Nel menu di spostamento superiore*** sono presenti quattro collegamenti attivi allineati nella sezione superiore della finestra principale *(Ti piace AVG?, Rapporti, Supporto, Opzioni).* Dettagli >>
- ***Informazioni sullo stato di protezione*** fornisce informazioni di base sullo stato corrente di **AVG Internet Security 2013**. Dettagli >>
- ***Nella striscia orizzontale di blocchi nella sezione centrale della finestra principale è possibile visualizzare la panoramica dei componenti installati***. I componenti vengono visualizzati come blocchi verde chiaro contrassegnati dall'icona e da informazioni sullo stato del relativo componente. Dettagli >>
- ***Le Applicazioni personali*** vengono visualizzate graficamente nella striscia centrale inferiore della finestra principale e offrono una panoramica delle applicazioni complementari ad **AVG Internet Security 2013**che sono già installate sul computer o che si consiglia di installare. Dettagli >>
- ***I collegamenti rapidi Scansione / Aggiornamento***sono posizionati nella riga di blocchi inferiore della finestra principale. Questi pulsanti consentono un accesso immediato alle funzionalità più importanti e più utilizzate di AVG. Dettagli >>

Al di fuori della finestra principale di **AVG Internet Security 2013** sono presenti altri due elementi di controllo che l'utente può utilizzare per accedere all'applicazione:

- ***L'icona della barra delle applicazioni*** è posizionata nell'angolo inferiore destro del monitor *(nella barra delle applicazioni)* e indica lo stato corrente di **AVG Internet Security 2013**. Dettagli >>

- ***Il gadget AVG*** è accessibile dalla sidebar di Windows (*supportata solo nei sistemi operativi Windows Vista/7/8*) e consente l'accesso rapido a scansioni e aggiornamenti in **AVG Internet Security 2013**. Dettagli >>

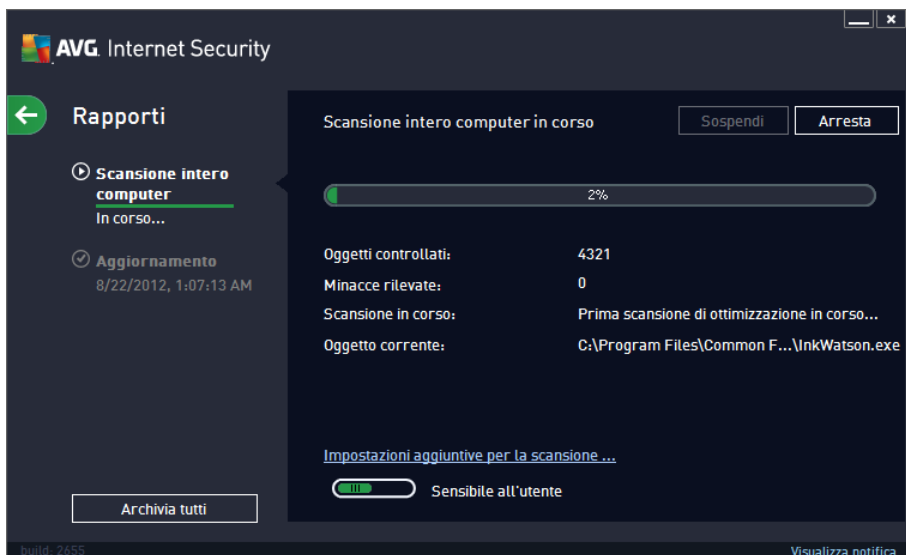
5.1. Menu di spostamento superiore

Nel ***menu di spostamento superiore*** sono presenti diversi collegamenti attivi allineati nella parte superiore della finestra principale. Il menu di spostamento include i seguenti pulsanti:

5.1.1. Ti piace AVG?

Fare clic sul collegamento per essere connessi alla comunità Facebook di AVG e condividere informazioni, novità e suggerimenti di AVG per la massima protezione di Internet.

5.1.2. Rapporti

Consente di aprire una nuova finestra di dialogo ***Rapporti*** con una panoramica di tutti i rapporti relativi alla scansioni avviate in precedenza e ai processi aggiornati. Se la scansione o l'aggiornamento è attualmente in esecuzione, verrà visualizzata un'icona rotante accanto al testo ***Rapporti*** nel menu di esplorazione superiore dell'interfaccia utente principale. Fare clic su tale icona per visualizzare nella finestra di dialogo l'avanzamento del processo in esecuzione:

5.1.3. Assistenza

Apre una nuova finestra di dialogo composta da quattro schede in cui è possibile trovare tutte le informazioni rilevanti su **AVG Internet Security 2013**:

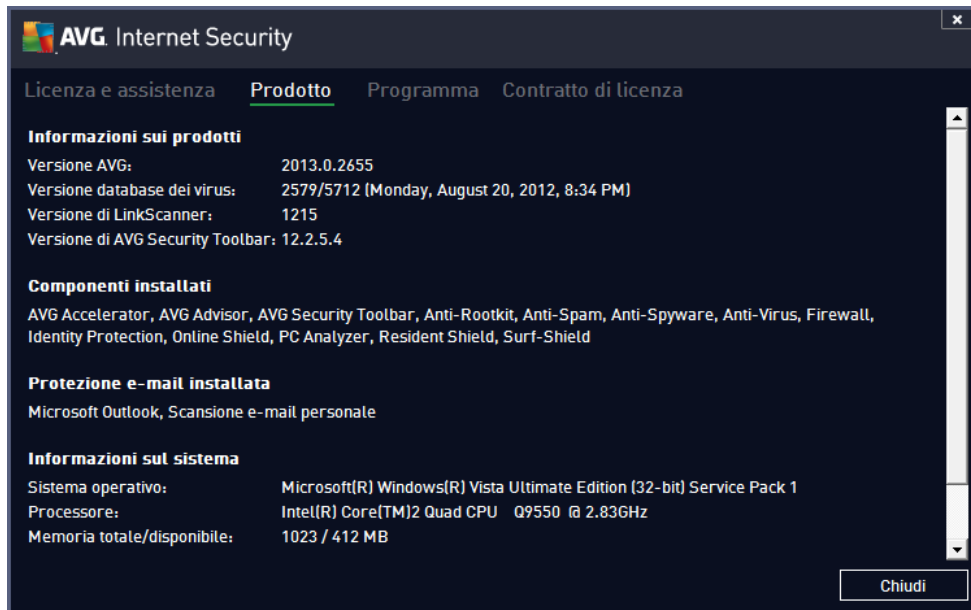
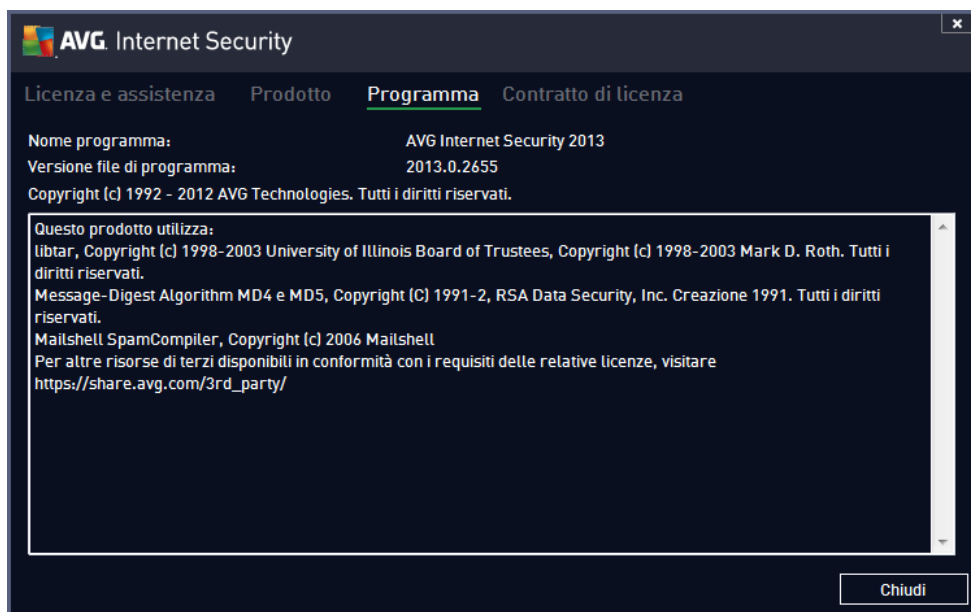
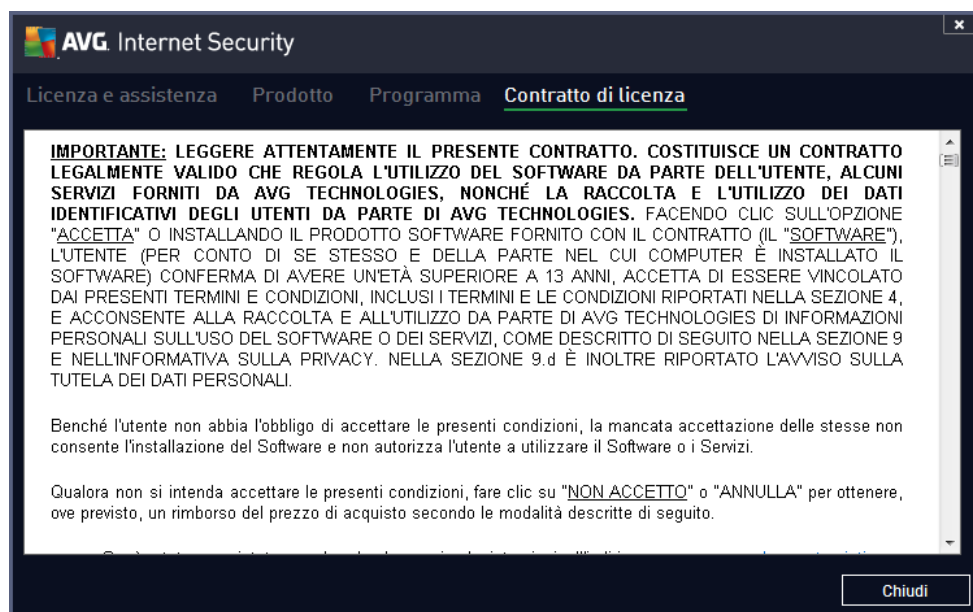
- ***Licenza e assistenza***: questa scheda fornisce le informazioni relative a nome prodotto, License Number e data di scadenza. Nella parte inferiore della finestra di dialogo è inoltre presente una panoramica organizzata in modo chiaro di tutti i contatti disponibili per

l'assistenza clienti. Nella scheda sono disponibili i seguenti pulsanti e collegamenti attivi:

- *(Ri)attiva*: fare clic per aprire la nuova finestra di dialogo ***Attiva software AVG***. Immettere il License Number nell'apposito campo per sostituire il Sales Number *(che si utilizza durante l'installazione di AVG Internet Security 2013)* oppure per cambiare il License Number corrente con un altro *(ad esempio quando si effettua l'upgrade a un prodotto AVG superiore)*.

- *Copia negli Appunti*: utilizzare questo collegamento per copiare il License Number e incollarlo dove necessario. In questo modo si sarà certi di immettere il License Number corretto.

- *Rinnova ora*: è consigliabile acquistare il rinnovo della licenza di **AVG Internet Security 2013** in anticipo, almeno un mese prima della scadenza della licenza corrente. L'utente verrà avvisato quando il periodo di licenza sta per scadere. Facendo clic su questo collegamento si viene reindirizzati al sito Web di AVG *(http://www.avg.com/)* in cui è possibile trovare informazioni dettagliate sullo stato della licenza, la data di scadenza e l'offerta di rinnovo/aggiornamento.

- ***Prodotto***: questa scheda presenta una panoramica dei dati tecnici più importanti di **AVG Internet Security 2013** relativi alle informazioni sul prodotto, ai componenti installati, alla protezione dei messaggi e-mail installata e alle informazioni sul sistema.

- ***Programma***: in questa scheda è possibile trovare informazioni sulla versione dei file di programma e sul codice di terzi utilizzato nel prodotto.

- ***Contratto di licenza***: in questa scheda è disponibile il testo completo del Contratto di licenza tra l'utente e AVG Technologies.

5.1.4. Opzioni

La manutenzione di **AVG Internet Security 2013** è accessibile tramite la voce ***Opzioni***. Fare clic sulla freccia per aprire il menu a discesa:

- ***Scansione computer*** avvia una scansione dell'intero computer.
- ***Scansione cartella selezionata...***: consente di passare all'interfaccia di scansione di AVG e di definire i file e le cartelle da sottoporre a scansione nella struttura del computer.
- ***Scansione file...***: consente di eseguire un controllo su richiesta di un singolo file specifico. Fare clic su questa opzione per aprire una nuova finestra con la struttura del disco. Selezionare il file desiderato e confermare l'avvio della scansione.
- ***Aggiorna***: avvia automaticamente il processo di aggiornamento di **AVG Internet Security 2013**.
- ***Aggiorna da directory...***: esegue il processo di aggiornamento dai file di aggiornamento che si trovano in una cartella specifica sul disco locale. Tuttavia, questa opzione è consigliabile solo in caso di emergenza, come in situazioni in cui non si ottiene la connessione a Internet (ad esempio, il computer è stato infettato e si è disconnesso da Internet, il computer è connesso a una rete senza accesso a Internet e così via). Nella finestra appena aperta selezionare la cartella in cui è stato precedentemente posizionato il file di aggiornamento e avviare il processo di aggiornamento.
- ***Quarantena virus***: consente di aprire l'interfaccia della finestra di quarantena (Quarantena virus) in cui AVG sposta tutte le infezioni rilevate che per qualche motivo non è possibile eliminare automaticamente. All'interno della quarantena i file infetti vengono isolati e la protezione del computer è garantita. Allo stesso tempo, i file infetti vengono archiviati per una possibile riparazione futura.
- ***Cronologia***: offre ulteriori opzioni specifiche nel sottomenu.

- *Risultati scansione*: consente di aprire una finestra di dialogo con una panoramica dei risultati della scansione.

- *Rilevamento Resident Shield*: consente di aprire una finestra di dialogo con una panoramica delle minacce rilevate da Resident Shield.

- *Rilevamento Protezione e-mail*: consente di aprire una finestra di dialogo con una panoramica degli allegati e-mail rilevati come pericolosi dal componente Protezione dei messaggi e-mail.

- *Rilevamenti di Online Shield*: consente di aprire una finestra di dialogo con una panoramica delle minacce rilevate da Online Shield.

- *Log cronologia eventi*: consente di aprire l'interfaccia di Log cronologia con una panoramica di tutte le azioni di **AVG Internet Security 2013** registrate.

- *Log Firewall*: consente di aprire una finestra di dialogo con una panoramica dettagliata di tutte le azioni del Firewall.

- ***Impostazioni avanzate...*** : consente di aprire la finestra di dialogo delle impostazioni AVG avanzate in cui è possibile modificare la configurazione di **AVG Internet Security 2013**. In genere è consigliabile mantenere le impostazioni dell'applicazione predefinite dal fornitore del software.

- ***Impostazioni del Firewall...***: consente di aprire una finestra di dialogo autonoma per la configurazione avanzata del componente Firewall.

- ***Sommario Guida***: consente di aprire i file della Guida di AVG.

- ***Ottieni assistenza***: consente di aprire il sito Web di AVG *(http://www.avg.com/)* nella pagina del centro di assistenza clienti.

- ***Web AVG personale***: consente di aprire il sito Web di AVG *(http://www.avg.com/).*

- ***Informazioni sui virus e le minacce***: consente di aprire l'Enciclopedia dei virus in linea in cui è possibile trovare informazioni dettagliate sul virus identificato.

- ***(Ri)attiva***: consente di aprire la finestra di dialogo ***Attiva AVG*** con i dati forniti durante il processo di installazione. In questa finestra di dialogo è possibile immettere il License Number per sostituire il Sales Number (*il numero con cui è stata eseguita l'installazione di AVG*) o il License Number in uso (*ad esempio, durante l'aggiornamento a un nuovo prodotto AVG*).

- ***Registra ora***: consente di connettersi alla pagina relativa alla registrazione del sito Web di AVG (http://www.avg.com/). Immettere i dati di registrazione. Solo i clienti che registrano il prodotto AVG possono ricevere assistenza tecnica gratuita. Se è in uso la versione di prova di **AVG Internet Security 2013**, le ultime due voci vengono visualizzate come ***Acquista ora*** e ***Attiva***, consentendo di acquistare subito la versione completa del programma. Se invece **AVG Internet Security 2013** è installato con un Sales Number, le voci vengono visualizzate come ***Registra*** e ***Attiva***.

- ***Informazioni su AVG***: consente di aprire una nuova finestra di dialogo con quattro schede in cui sono presenti i dati sul tipo di licenza acquistata e le informazioni disponibili

sull'assistenza, il prodotto e il programma, oltre al testo completo del Contratto di licenza.

5.2. Informazioni sullo stato di protezione

La sezione ***Informazioni sullo stato di protezione*** si trova nella parte superiore della finestra principale di **AVG Internet Security 2013**. All'interno di questa sezione sono contenute le informazioni sullo stato di protezione corrente di **AVG Internet Security 2013**. Vedere la panoramica delle icone eventualmente visualizzate in questa sezione, con il relativo significato:

: l'icona verde indica che ***AVG Internet Security 2013 è completamente funzionante***. Il computer è totalmente protetto, aggiornato e tutti i componenti installati funzionano correttamente.

: l'icona gialla indica ***la configurazione non corretta di uno o più componenti***. È consigliabile controllare le relative proprietà/impostazioni. Non sono presenti problemi gravi in **AVG Internet Security 2013** e probabilmente si è deciso di disattivare alcuni componenti per qualche ragione. La protezione è comunque attiva. Tuttavia, prestare attenzione alle impostazioni del componente in cui si sono verificati problemi. Il componente configurato in modo errato verrà visualizzato con una striscia arancione di avviso nell'interfaccia utente principale.

L'icona gialla viene inoltre visualizzata se, per qualche motivo, l'utente ha deciso di ignorare lo stato di errore di un componente. L'opzione ***Ignora lo stato di errore*** è accessibile nel ramo Impostazioni avanzate / Ignora stato di errore. Qui è presente l'opzione per confermare che si è al corrente dello stato di errore del componente, tuttavia si desidera mantenere **AVG Internet Security 2013** nella condizione attuale e non si desidera ricevere notifiche a riguardo. Potrebbe essere necessario utilizzare l'opzione ***Ignora stato del componente*** in situazioni particolari, tuttavia si consiglia di disattivare questa opzione nel più breve tempo possibile.

In alternativa, l'icona gialla verrà visualizzata anche se **AVG Internet Security 2013** richiede il riavvio del computer (***Riavvio necessario***). Prestare attenzione all'avviso e riavviare il PC.

: l'icona arancione indica che ***AVG Internet Security 2013 si trova in uno stato critico***. Uno o più componenti non funzionano correttamente e **AVG Internet Security 2013** non è in grado di proteggere il computer. Intervenire immediatamente per risolvere il problema segnalato! Se non si è in grado di correggere l'errore, contattare il team dell'Assistenza tecnica di AVG.

Se AVG Internet Security 2013 non è impostato per prestazioni ottimali, un nuovo pulsante denominato Fare clic per risolvere il problema (oppure Fare clic per risolvere i problemi se il problema riguarda più componenti) appare accanto alle informazioni sullo stato della protezione. Selezionare il pulsante per avviare un processo automatico di controllo e configurazione del programma. Questo è un modo rapido per impostare AVG Internet Security 2013 per prestazioni ottimali e ottenere il livello di protezione massimo.

Si consiglia di prestare attenzione alla sezione ***Informazioni sullo stato di protezione*** e, nel caso in cui fosse segnalato un problema, procedere cercando di risolverlo immediatamente. In caso contrario, il computer è a rischio.

Nota: *le informazioni sullo stato di AVG Internet Security 2013 sono inoltre sempre disponibili*

tramite l'icona della barra delle applicazioni.

5.3. Panoramica dei componenti

La ***panoramica dei componenti installati*** è disponibile nella striscia orizzontale di blocchi nella sezione centrale della finestra principale. Questi componenti vengono visualizzati come blocchi verde chiaro contrassegnati dall'icona del relativo componente. Ogni blocco fornisce informazioni sullo stato corrente della protezione. Se il componente viene configurato correttamente ed è completamente funzionante, l'informazione viene riportata in caratteri verdi. Se il componente viene arrestato e la relativa funzionalità viene limitata o se il componente si trova in stato di errore, l'utente verrà informato tramite un messaggio di avviso visualizzato in un campo di testo arancione. ***Si consiglia di prestare attenzione alle relative impostazioni del componente.***

Spostare il puntatore sul componente per visualizzare un breve testo nella parte inferiore della finestra principale. Il testo fornisce un'introduzione di base alla funzionalità del componente. Comunica inoltre lo stato corrente del componente e specifica quale servizio del componente non è configurato correttamente.

Elenco dei componenti installati

In **AVG Internet Security 2013** la sezione ***Panoramica dei componenti*** contiene informazioni sui seguenti componenti:

- ***Computer***: questo componente comprende due servizi, ovvero ***Anti-Virus Shield*** , in grado di rilevare virus, spyware, worm, trojan, librerie o file eseguibili indesiderati presenti nel sistema e di proteggere da adware dannoso e***Anti-Rootkit***, in grado di ricercare i rootkit pericolosi nascosti in applicazioni, driver o librerie. Dettagli >>
- ***Esplorazione Web***: protegge da attacchi basati sul Web durante le ricerche e la navigazione in Internet. Dettagli >>
- ***Identity***: questo componente esegue il servizio ***Identity Shield*** che protegge in modo costante le risorse digitali da minacce nuove e sconosciute in Internet. Dettagli >>
- ***E-mail***: controlla la presenza di SPAM nei messaggi e-mail in arrivo e blocca virus, attacchi di phishing o altre minacce. Dettagli >>
- ***Firewall***: controlla tutte le comunicazioni in tutte le porte di rete, proteggendo il PC da attacchi pericolosi e bloccando tutti i tentativi di intrusione. Dettagli >>

Azioni accessibili

- ***Posizionare il mouse sull'icona di un componente*** per evidenziarlo all'interno della panoramica dei componenti. Contemporaneamente, viene visualizzata la descrizione delle funzionalità di base del componente nella parte inferiore dell'interfaccia utente.
- ***Fare clic sull'icona del componente*** per aprire l'interfaccia con le informazioni relative allo stato corrente e accedere alla configurazione e ai dati statistici del componente.

5.4. Applicazioni personali

Nell'area ***Applicazioni personali*** *(la riga di blocchi verdi sotto il gruppo dei componenti)* è possibile trovare una panoramica di ulteriori applicazioni di AVG che sono pronte per essere installate sul computer o che si consiglia di installare. I blocchi vengono visualizzati in modo condizionale e possono rappresentare una delle seguenti applicazioni:

- ***Protezione mobile*** è un'applicazione che protegge il cellulare da virus e malware. Fornisce inoltre la capacità di rilevare lo smartphone in modalità remota in caso di necessità.
- ***LiveKive*** è destinato al backup dei dati in linea su server sicuri. LiveKive esegue il backup automatico di tutti i file, le foto e la musica in una posizione sicura, consentendo di condividerli con familiari e amici e di accedervi da qualsiasi dispositivo abilitato per il Web, inclusi dispositivi Android e iPhone.
- ***Family Safety*** consente di proteggere i bambini da siti Web, ricerche in linea e contenuti multimediali inappropriati e fornisce rapporti relativi alle attività che essi svolgono in linea. AVG Family Safety utilizza tecnologie di monitoraggio della pressione dei tasti per controllare le attività dei bambini nelle chat room e nei social network. Se rileva parole, frasi o espressioni tipicamente utilizzati per adescare i bambini in linea, invia una notifica immediata tramite SMS o e-mail. L'applicazione consente di impostare il livello di protezione che meglio si adatta a ciascun bambino e controllarne l'attività separatamente tramite dati di accesso univoci.
- ***PC Tuneup*** è uno strumento avanzato per l'analisi e la correzione dettagliate del sistema che consente di migliorare la velocità e le prestazioni generali del computer.
- ***MultiMi*** raccoglie tutti gli account e-mail e dei social network in una posizione sicura semplificando i contatti con famiglia e amici, l'esplorazione in Internet e la condivisione di foto, video e file. MultiMi include il servizio LinkScanner che protegge l'utente dal numero crescente di minacce nel Web analizzando le pagine Web dietro a tutti i collegamenti presenti sulla pagina Web visualizzata e garantendo che le pagine siano sicure.
- ***AVG Toolbar*** è disponibile direttamente nel browser Internet per assicurare la protezione massima durante l'esplorazione in Internet.

Per informazioni dettagliate sulle applicazioni di ***Applicazioni personali*** fare clic sul relativo blocco. Si verrà reindirizzati alla pagina Web di AVG dedicata, da cui è possibile scaricare immediatamente il componente.

5.5. Collegamenti rapidi Scansione / Aggiornamento

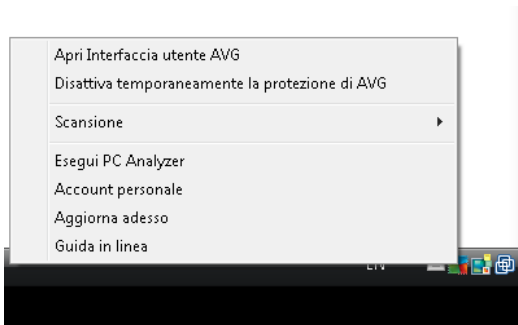
I ***collegamenti rapidi*** si trovano nella parte sinistra dell'interfaccia utente di **AVG Internet Security 2013**. Questi collegamenti consentono di accedere immediatamente alle funzionalità più importanti e più utilizzate dell'applicazione, ossia scansione e aggiornamento. I collegamenti rapidi sono accessibili da tutte le finestre di dialogo dell'interfaccia utente:

- ***Esegui scansione***: questo pulsante è diviso graficamente in due sezioni. Selezionare il collegamento ***Esegui scansione*** per avviare subito la Scansione intero computer e visualizzare l'avanzamento e risultati relativi nella finestra Rapporti aperta automaticamente. Il pulsante ***Opzioni*** apre la finestra di dialogo ***Opzioni di scansione*** in cui è possibile gestire le scansioni pianificate e modificare i parametri di Scansione intero computer /

Scansione file o cartelle. *Per dettagli, vedere il capitolo Scansione AVG.*

- ***Aggiorna adesso***: premere il pulsante per avviare subito l'aggiornamento del prodotto. È possibile visualizzare l'avanzamento e i risultati dell'aggiornamento nella finestra ***Rapporti*** aperta automaticamente. *Per dettagli, vedere il capitolo Aggiornamenti di AVG.*

5.6. Icona della barra delle applicazioni

L'***icona della barra delle applicazioni di AVG*** *(presente nella barra delle applicazioni di Windows, nell'angolo inferiore destro dello schermo)* indica lo stato corrente di **AVG Internet Security 2013**. È possibile visualizzarla in qualsiasi momento sulla barra delle applicazioni, indipendentemente dall'apertura o meno dell'interfaccia utente di **AVG Internet Security 2013**:

Aspetto dell'icona della barra delle applicazioni di AVG

- Se è completamente colorata e non presenta elementi aggiunti, l'icona indica che tutti i componenti di **AVG Internet Security 2013** sono attivi e funzionano correttamente. Tuttavia, l'icona può venire visualizzata in questo modo anche quando uno dei componenti non è completamente funzionante ma l'utente ha deciso di ignorare lo stato del componente. *Selezionando l'opzione Ignora stato del componente si conferma di essere al corrente dello stato di errore del componente, tuttavia si desidera mantenere la condizione attuale e non si desidera ricevere notifiche a riguardo.*

- L'icona con un punto esclamativo indica che un componente *o più componenti* si trovano in uno stato di errore. Prestare sempre attenzione a tale avviso e tentare di rimuovere il problema di configurazione del componente non impostato correttamente. Per modificare la configurazione del componente, fare doppio clic sull'icona della barra delle applicazioni per aprire l'interfaccia utente dell'applicazione. Per informazioni dettagliate sui componenti in stato di errore, consultare la sezione relativa alle informazioni sullo stato di protezione.

- L'icona della barra delle applicazioni può venire inoltre visualizzata completamente colorata con un fascio di luce rotante. Questa versione grafica segnala l'avvio di un processo di aggiornamento.

- La visualizzazione alternativa dell'icona completamente colorata con una freccia centrale indica che è in esecuzione una scansione di **AVG Internet Security 2013**.

Informazioni sull'icona della barra delle applicazioni di AVG

L'***icona della barra delle applicazioni di AVG*** informa inoltre l'utente circa attività correnti in **AVG Internet Security 2013** ed eventuali modifiche dello stato del programma (*ad esempio avvio automatico di una scansione o un aggiornamento pianificato, variazione del profilo Firewall, modifica dello stato di un componente, occorrenza di uno stato di errore e così via*) tramite una finestra popup che si apre dall'icona stessa:

Azioni accessibili tramite l'icona della barra delle applicazioni di AVG

L'***icona della barra delle applicazioni di AVG*** può inoltre essere utilizzata come collegamento rapido per accedere all'interfaccia utente di **AVG Internet Security 2013**, semplicemente tramite doppio clic. Se si fa clic con il pulsante destro del mouse sull'icona, viene aperto un menu di scelta rapida contenente le seguenti opzioni:

- ***Apri interfaccia utente di AVG***: fare clic per aprire l'interfaccia utente di **AVG Internet Security 2013**.

- ***Disattiva temporaneamente la protezione AVG***: questa opzione consente di disattivare completamente la protezione assicurata da **AVG Internet Security 2013**. Non utilizzare questa opzione se non è assolutamente necessario. Nella maggior parte dei casi, non è necessario disattivare **AVG Internet Security 2013** prima di installare nuovi software o driver, neppure se il programma di installazione o la procedura guidata suggeriscono di chiudere tutti i programmi e le applicazioni in esecuzione per accertarsi che non si verifichino interruzioni indesiderate durante il processo di installazione. Se fosse necessario disattivare temporaneamente **AVG Internet Security 2013**, lo si dovrà riattivare non appena possibile. Se si è connessi a Internet o a una rete mentre il software antivirus è disattivato, il computer sarà esposto a potenziali attacchi.

- ***Scansione***: fare clic per aprire il menu di scelta rapida delle scansioni predefinite (*Scansione intero computer* e *Scansione file o cartelle*) e selezionare la scansione richiesta, che verrà avviata immediatamente.

- ***Esecuzione delle scansioni in corso...***: questa voce viene visualizzata solo se una scansione è in esecuzione sul computer. Per questa scansione è possibile impostare la priorità oppure arrestarla o sospenderla. Inoltre, sono accessibili le seguenti azioni: *Imposta priorità per tutte le scansioni, Sospendi tutte le scansioni* o *Arresta tutte le scansioni*.

- ***Esegui PC Analyzer***: fare clic per avviare il componente PC Analyzer.

- ***Account personale***: apre la pagina iniziale dell'Account personale in cui è possibile gestire i prodotti con sottoscrizione, acquistare una protezione aggiuntiva, scaricare i file di installazione, controllare gli ordini e le fatture precedenti e gestire le informazioni personali.

- ***Aggiorna adesso***: viene avviato un aggiornamento immediato.

- ***Guida in linea***: apre il file della Guida alla pagina iniziale.

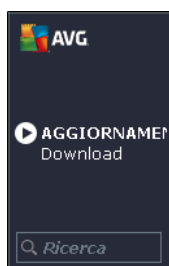
5.7. Gadget AVG

Il ***gadget AVG*** viene visualizzato sul desktop di Windows (*sidebar di Windows*). Questa applicazione è supportata solo sui sistemi operativi Windows Vista e Windows 7/8. Il ***gadget AVG*** offre l'accesso immediato alla funzionalità più importante di **AVG Internet Security 2013** , ovvero scansione e aggiornamento:

Controlli del gadget AVG

Se necessario, il gadget AVG consente di avviare immediatamente una scansione o un aggiornamento. Fornisce inoltre un collegamento rapido per la connessione ai principali social network e uno strumento per la ricerca rapida:

- ***Esegui scansione***: fare clic sul collegamento ***Esegui scansione*** per avviare direttamente la scansione intero computer. È possibile visualizzare l'avanzamento del processo di scansione nell'interfaccia utente alternativa del gadget. Una breve panoramica delle statistiche fornisce informazioni sul numero di oggetti esaminati, minacce rilevate e minacce corrette. È possibile sospendere o arrestare il processo di scansione in corso in qualsiasi momento. Per dati dettagliati relativi ai risultati di scansione, consultare la finestra di dialogo standard Panoramica risultati di scansione che può essere aperta direttamente dal gadget tramite l'opzione ***Mostra dettagli*** *(i risultati di scansione pertinenti verranno elencati alla voce Scansione gadget sidebar)*.

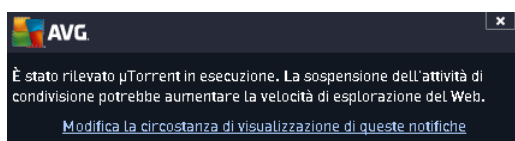
- ***Aggiorna adesso***: fare clic sul collegamento ***Aggiorna adesso*** per avviare l'aggiornamento di **AVG Internet Security 2013** direttamente dal gadget:

- ***Collegamento Twitter*** : apre una nuova interfaccia del ***gadget AVG*** che fornisce una panoramica dei feed AVG più recenti pubblicati in Twitter. Seguire il collegamento ***Visualizza tutti i feed Twitter di AVG*** per aprire il browser Internet in una nuova finestra e passare direttamente al sito Web Twitter, in corrispondenza della pagina dedicata alle notizie relative ad AVG.

- ***Collegamento Facebook*** : apre il browser Internet sul sito Web Facebook, in corrispondenza della pagina dedicata alla ***community AVG***.

- ***Casella di ricerca***: digitare una parola chiave per ottenere subito i risultati della ricerca in una nuova finestra del browser Web predefinito.

5.8. AVG Advisor

AVG Advisor è stato progettato per rilevare i problemi che potrebbero causare un rallentamento del computer o metterne a rischio la protezione e raccomandare una soluzione. Se si verifica un improvviso rallentamento del computer *(esplorazione di Internet, prestazioni complessive)*, generalmente non è facile capire quale sia la causa del problema e quindi come risolverlo. In questo caso, ***AVG Advisor*** visualizza una notifica sulla barra delle applicazioni che segnala il possibile problema e suggerisce come risolverlo. ***AVG Advisor*** controlla continuamente tutti i processi in esecuzione nel PC in cerca di possibili problemi e offre suggerimenti utili per evitare il problema.

AVG Advisor è visualizzato sotto forma di una finestra popup che compare sulla barra delle applicazioni:

In particolare, ***AVG Advisor*** monitora i seguenti elementi:

- ***Lo stato dei browser Web attualmente aperti***. I browser Web possono sovraccaricare la memoria, in particolare se si lasciano aperte per diverso tempo più schede o finestre, e utilizzare una quantità eccessiva di risorse di sistema, rallentando il computer. In tali situazioni, in genere è consigliabile riavviare il browser Web.

- ***Esecuzione di connessioni peer-to-peer***. Dopo l'utilizzo del protocollo P2P per la condivisione di file, talvolta la connessione può rimanere attiva utilizzando una certa quantità di larghezza di banda. Di conseguenza, può verificarsi un rallentamento dell'esplorazione Web.

- ***Reti sconosciute con un nome familiare***. Questa situazione in genere si applica solo agli utenti che si connettono a varie reti, solitamente con computer portatili. Se una nuova rete sconosciuta ha lo stesso nome di una rete conosciuta e utilizzata di frequente*(ad esempio Casa o Wifi)*, l'utente potrebbe collegarsi accidentalmente a una rete completamente sconosciuta e potenzialmente non sicura. ***AVG Advisor*** può impedire questa situazione segnalando che la rete apparentemente nota è in realtà una nuova rete. Naturalmente, se si decide che la rete sconosciuta è sicura, è possibile salvarla in un elenco di reti note di ***AVG Advisor*** , in modo che non venga più segnalata in futuro.

In tutti questi casi, ***AVG Advisor*** comunica la presenza di possibili problemi e fornisce il nome e l'icona del processo o dell'applicazione in conflitto. Inoltre, ***AVG Advisor*** suggerisce la procedura da eseguire per evitare i possibili problemi.

Browser Web supportati

La funzionalità è utilizzabile con i seguenti browser Web:Internet Explorer, Chrome, Firefox, Opera, Safari.

5.9. AVG Accelerator

AVG Accelerator ottimizza la riproduzione dei video in linea e semplifica il download. Quando il processo di accelerazione video è in corso, l'utente ne verrà informato tramite la finestra a comparsa sulla barra delle applicazioni.

6. Componenti di AVG

6.1. Computer

Il componente ***Computer***comprende due servizi di protezione principali: ***Anti-Virus*** e ***Anti-Rootkit***.

- ***Anti-Virus*** è costituito da un motore di scansione che controlla tutti i file, le aree di sistema del computer e i supporti rimovibili *(unità flash e così via)* e ricerca i virus noti. Tutti i virus rilevati verranno bloccati per essere poi corretti o messi in Quarantena virus. Questo processo non viene notato dall'utente, poiché la protezione permanente viene eseguita "in background". Anti-Virus utilizza anche la scansione euristica, che consente di rilevare le caratteristiche tipiche dei virus. In questo modo Anti-Virus è in grado di rilevare un nuovo virus sconosciuto, se tale virus contiene alcune caratteristiche tipiche dei virus esistenti. **AVG Internet Security 2013** è inoltre in grado di analizzare e rilevare le applicazioni eseguibili o le librerie DLL che potrebbero essere potenzialmente indesiderate nel sistema *(vari tipi di spyware, adware e così via)*. Inoltre, Anti-Virus esegue la scansione del Registro di sistema alla ricerca di voci sospette, file Internet temporanei e cookie di tracciamento e consente di trattare tutti gli elementi potenzialmente dannosi come avviene per le altre infezioni.

- ***Anti-Rootkit*** è uno strumento specializzato per il rilevamento e la rimozione efficace di rootkit dannosi, ossia programmi e tecnologie che possono camuffare la presenza di software dannoso nel computer. Un rootkit è progettato per assumere il controllo di base di un sistema senza autorizzazione da parte dei proprietari e dei gestori legittimi del sistema. Anti-Rootkit è in grado di rilevare i rootkit in base a un gruppo di regole predefinito. Se Anti-Rootkit rileva un rootkit, ciò non significa necessariamente che il rootkit sia infetto. Talvolta i rootkit vengono utilizzati come driver o fanno parte di applicazioni regolari.

Comandi della finestra di dialogo

Per passare da una sezione all'altra della finestra di dialogo, è possibile fare clic in qualsiasi punto del rispettivo pannello di servizio. Il pannello viene evidenziato in una tonalità di blu più chiara. In entrambe le sezioni della finestra di dialogo è possibile trovare i seguenti controlli. La funzionalità è la stessa, indipendentemente dal servizio di protezione a cui appartengono *(Anti-Virus o Anti-Rootkit)*:

Attivato / Disattivato : questo pulsante è simile a un semaforo, sia nell'aspetto che nella funzionalità. Fare clic per passare da una posizione all'altra. Il colore verde significa ***Attivato***, ovvero indica che il servizio di protezione Anti-Virus è attivo e completamente funzionante. Il colore rosso rappresenta lo stato ***Disattivato*** , ovvero indica che il servizio è disabilitato. A meno che non sussista un motivo valido per disattivare il servizio, si consiglia di mantenere le impostazioni predefinite per tutte le configurazioni di protezione. Le impostazioni predefinite assicurano prestazioni ottimali dell'applicazione e massima protezione. Se per qualche ragione si desidera disattivare il servizio, per mettere in guardia dai possibili rischi verrà subito visualizzato il simbolo rosso di ***Avviso*** e l'utente verrà informato che la protezione non è completa. ***Tenere presente che è necessario riattivare il servizio il prima possibile.***

Impostazioni: facendo clic su questo pulsante si viene reindirizzati all'area delle impostazioni avanzate. Verrà aperta la relativa finestra di dialogo e sarà possibile configurare il servizio selezionato, ovvero Anti-Virus o Anti-Rootkit. Nell'area delle impostazioni avanzate è possibile modificare la configurazione di ogni servizio di protezione tramite **AVG Internet Security 2013**, tuttavia le eventuali modifiche sono consigliate ai soli utenti esperti.

Statistiche : facendo clic su questo pulsante si viene reindirizzati alla pagina dedicata nel sito web di AVG (http://www.avg.com/). In tale pagina è disponibile una panoramica statistica dettagliata di tutte le attività di **AVG Internet Security 2013** eseguite sul computer in uno specifico periodo di tempo e in totale.

Dettagli: facendo clic su questo pulsante, nella parte inferiore della finestra di dialogo verrà visualizzata una breve descrizione del servizio evidenziato.

: usare la freccia verde nella parte superiore sinistra della finestra di dialogo per tornare all' interfaccia utente principale con la panoramica dei componenti.

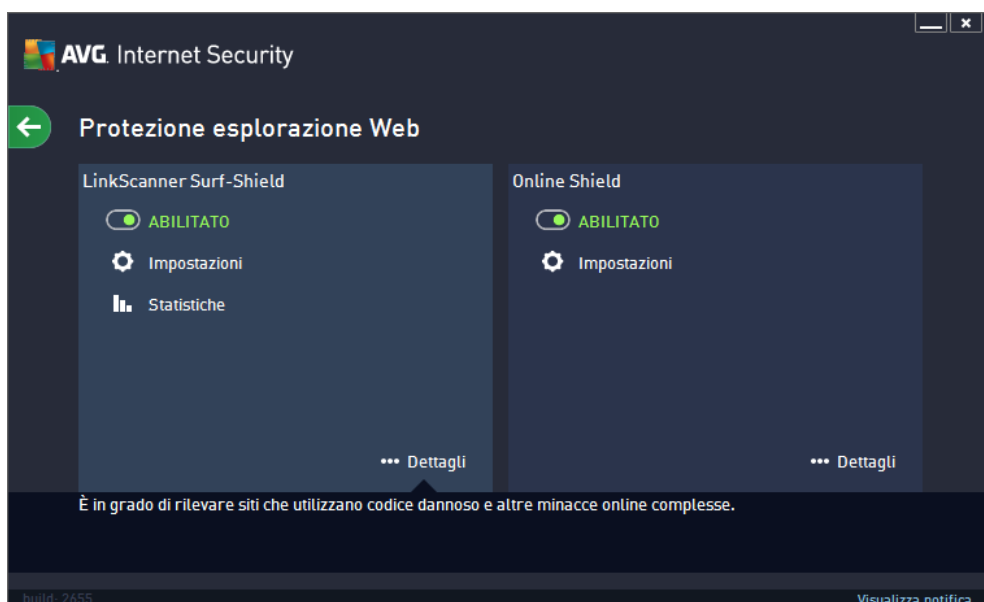
Nella sezione Anti-Rootkit è presente anche un pulsante specifico ***Ricerca di rootkit*** che può essere utilizzato per avviare direttamente la ricerca indipendente di rootkit *(tuttavia, la scansione rootkit è inclusa nella Scansione intero computer)*.

6.2. Esplorazione Web

La ***Protezione della navigazione sul Web*** è composta da due servizi: ***LinkScanner Surf-Shield*** e ***Online Shield***.

- ***LinkScanner Surf-Shield*** protegge dal numero sempre crescente di minacce transitorie presenti sul Web. Queste minacce possono nascondersi in qualsiasi tipo di sito Web, da quelli degli enti governativi, a quelli di grandi marchi famosi, a quelli di piccole aziende, e raramente restano in questi siti per più di 24 ore. LinkScanner protegge gli utenti analizzando le pagine Web dietro a tutti i collegamenti presenti sulla pagina Web visualizzata e garantendo che le pagine siano sicure nel momento cruciale, ovvero nell'attimo in cui si sta per fare clic sul collegamento. ***Il componente LinkScanner Surf-***

Shield non è destinato alla protezione delle piattaforme server.

- ***Online Shield*** è un tipo di protezione permanente in tempo reale che esegue la scansione del contenuto delle pagine Web visitate (e dei possibili file in esse contenuti) persino prima che vengano visualizzate nel browser Web o scaricate nel computer. Online Shield rileva se la pagina che sta per essere aperta contiene javascript dannosi e ne impedisce la visualizzazione. Inoltre, riconosce il malware contenuto in una pagina arrestandone immediatamente il download per impedirne il trasferimento nel computer. Si tratta di un potente strumento di protezione che blocca il contenuto pericoloso delle pagine Web quando si tenta di aprirle, impedendone il download sul computer. Se questa funzionalità è abilitata, quando si fa clic sul collegamento o si digita l'URL di un sito pericoloso, l'apertura della pagina Web verrà bloccata immediatamente impedendo che il PC dell'utente venga infettato. È importante tenere presente che le pagine Web dannose possono infettare il computer con il semplice accesso al sito infetto. ***Il componente Online Shield non è destinato alle piattaforme server.***

Comandi della finestra di dialogo

Per passare da una sezione all'altra della finestra di dialogo, è possibile fare clic in qualsiasi punto del rispettivo pannello di servizio. Il pannello viene evidenziato in una tonalità di blu più chiara. In entrambe le sezioni della finestra di dialogo è possibile trovare i seguenti controlli. La funzionalità è la stessa, indipendentemente dal servizio di protezione a cui appartengono *(LinkScanner Surf-Shield o Online Shield)*:

Attivato / Disattivato : questo pulsante è simile a un semaforo, sia nell'aspetto che nella funzionalità. Fare clic per passare da una posizione all'altra. Il colore verde significa ***Attivato***, ovvero indica che il servizio di protezione LinkScanner Surf-Shield / Online Shield è attivo e completamente funzionante. Il colore rosso rappresenta lo stato ***Disattivato*** , ovvero indica che il servizio è disabilitato. A meno che non sussista un motivo valido per disattivare il servizio, si consiglia di mantenere le impostazioni predefinite per tutte le configurazioni di protezione. Le impostazioni predefinite assicurano prestazioni ottimali dell'applicazione e massima protezione. Se per qualche ragione si desidera disattivare il servizio, per mettere in

guardia dai possibili rischi verrà subito visualizzato il simbolo rosso di ***Avviso*** e l'utente verrà informato che la protezione non è completa. ***Tenere presente che è necessario riattivare il servizio il prima possibile.***

Impostazioni: facendo clic su questo pulsante si viene reindirizzati all'area delle impostazioni avanzate. Più precisamente, verrà aperta la rispettiva finestra di dialogo e l'utente potrà configurare il servizio selezionato, ovvero LinkScanner Surf-Shield o Online Shield. Nell'area delle impostazioni avanzate è possibile modificare la configurazione di ogni servizio di protezione tramite **AVG Internet Security 2013**, tuttavia le eventuali modifiche sono consigliate ai soli utenti esperti.

Statistiche : facendo clic su questo pulsante si viene reindirizzati alla pagina dedicata nel sito web di AVG (http://www.avg.com/). In tale pagina è disponibile una panoramica statistica dettagliata di tutte le attività di **AVG Internet Security 2013** eseguite sul computer in uno specifico periodo di tempo e in totale.

Dettagli: facendo clic su questo pulsante, nella parte inferiore della finestra di dialogo verrà visualizzata una breve descrizione del servizio evidenziato.

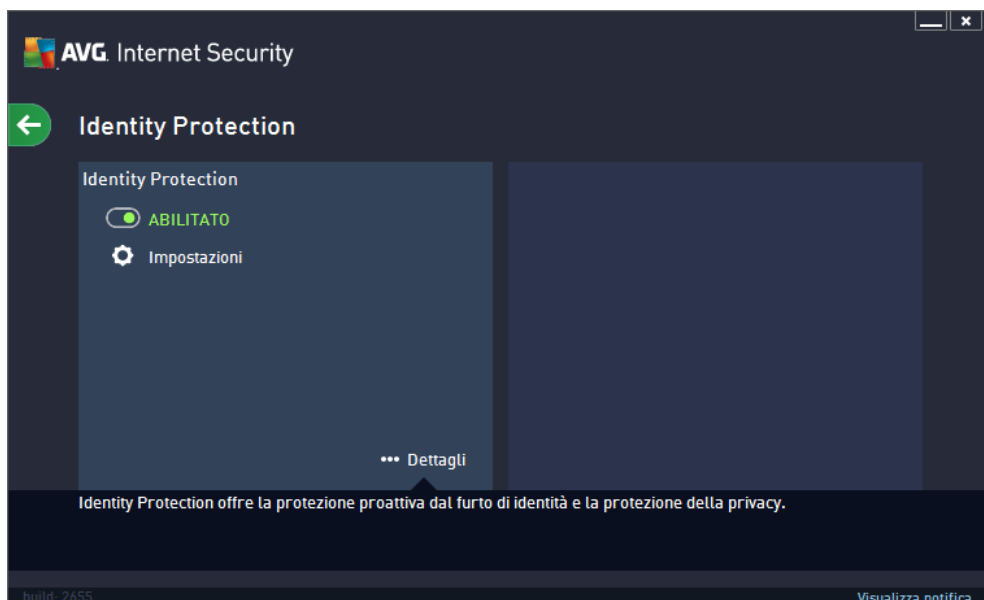
: usare la freccia verde nella parte superiore sinistra della finestra di dialogo per tornare all' interfaccia utente principale con la panoramica dei componenti.

6.3. Identity

Il componente ***Identity Protection*** è costituito da due servizi:***Identity Protection***e ***Identity Alert***.

- ***Identity Protection*** è un servizio anti-malware che protegge da tutti i tipi di malware (*spyware, bot, furto di identità e così via*) utilizzando tecnologie basate sul comportamento e fornisce la protezione zero day per i nuovi virus. Identity Protection è destinato alla prevenzione di attacchi da parte di malintenzionati volti a sottrarre password, dati dei conti bancari, numeri delle carte di credito e altri importanti dati digitali tramite qualsiasi tipo di software dannoso *(malware)* in grado di colpire il PC. L'applicazione assicura che tutti i programmi in esecuzione nel PC o nella rete condivisa funzionino correttamente. Identity Protection rileva e blocca i comportamenti sospetti e protegge il computer da tutti i nuovi malware. Identity Protection fornisce al computer la protezione in tempo reale da minacce nuove e sconosciute. Monitora tutti i processi *(compresi quelli nascosti) e oltre 285 diversi schemi di comportamento ed è in grado di determinare se nel sistema si stanno verificando operazioni dannose.* Per tale motivo, può rilevare minacce non ancora descritte nel database dei virus. Quando un codice sconosciuto entra nel computer viene immediatamente controllato, per verificarne l'eventuale comportamento dannoso, e tracciato. Se si determina che il file è dannoso, Identity Protection rimuove il codice spostandolo in Quarantena virus e annulla le modifiche apportate al sistema *(iniezioni di codice, modifiche del registro, apertura di porte e così via)*. Non è necessario avviare una scansione per essere protetti. La tecnologia è proattiva, richiede raramente l'aggiornamento ed è sempre attiva.

- ***Identity Alert*** fornisce l'accesso a un servizio basato sul Web progettato per monitorare in modo discreto i dati personali in linea. I dati possono includere: numero della carta di credito, indirizzo e-mail, numero di telefono *(cellulare)* e così via. Il monitoraggio viene effettuato in modo continuo verificando che i dati non siano stati oggetto di potenziali usi impropri. Se il servizio rileva un'attività sospetta, l'utente riceve una comunicazione via e-

mail. Poiché il servizio è basato sul Web e funziona solo in linea, sarà necessario essere connessi a Internet per accedere al componente Identity Alert.

Comandi della finestra di dialogo

Per passare da una sezione all'altra della finestra di dialogo, è possibile fare clic in qualsiasi punto del rispettivo pannello di servizio. Il pannello viene evidenziato in una tonalità di blu più chiara. In entrambe le sezioni della finestra di dialogo è possibile trovare i seguenti controlli. La funzionalità è la stessa, indipendentemente dal servizio di protezione a cui appartengono *(Identity Protection o Identity Alert)*:

Attivato / Disattivato : questo pulsante è simile a un semaforo, sia nell'aspetto che nella funzionalità. Fare clic per passare da una posizione all'altra. Il colore verde significa ***Attivato***, ovvero indica che il servizio di protezione Identity Protection è attivo e completamente funzionante. Il colore rosso rappresenta lo stato ***Disattivato*** , ovvero indica che il servizio è disabilitato. A meno che non sussista un motivo valido per disattivare il servizio, si consiglia di mantenere le impostazioni predefinite per tutte le configurazioni di protezione. Le impostazioni predefinite assicurano prestazioni ottimali dell'applicazione e massima protezione. Se per qualche ragione si desidera disattivare il servizio, per mettere in guardia dai possibili rischi verrà subito visualizzato il simbolo rosso di ***Avviso*** e l'utente verrà informato che la protezione non è completa. ***Tenere presente che è necessario riattivare il servizio il prima possibile.***

Impostazioni: facendo clic su questo pulsante si viene reindirizzati all'area delle impostazioni avanzate. Verrà aperta la relativa finestra di dialogo e sarà possibile configurare il servizio selezionato, ovvero Identity Protection. Nell'area delle impostazioni avanzate è possibile modificare la configurazione di ogni servizio di protezione tramite **AVG Internet Security 2013**, tuttavia le eventuali modifiche sono consigliate ai soli utenti esperti.

Dettagli: facendo clic su questo pulsante, nella parte inferiore della finestra di dialogo verrà visualizzata una breve descrizione del servizio evidenziato.

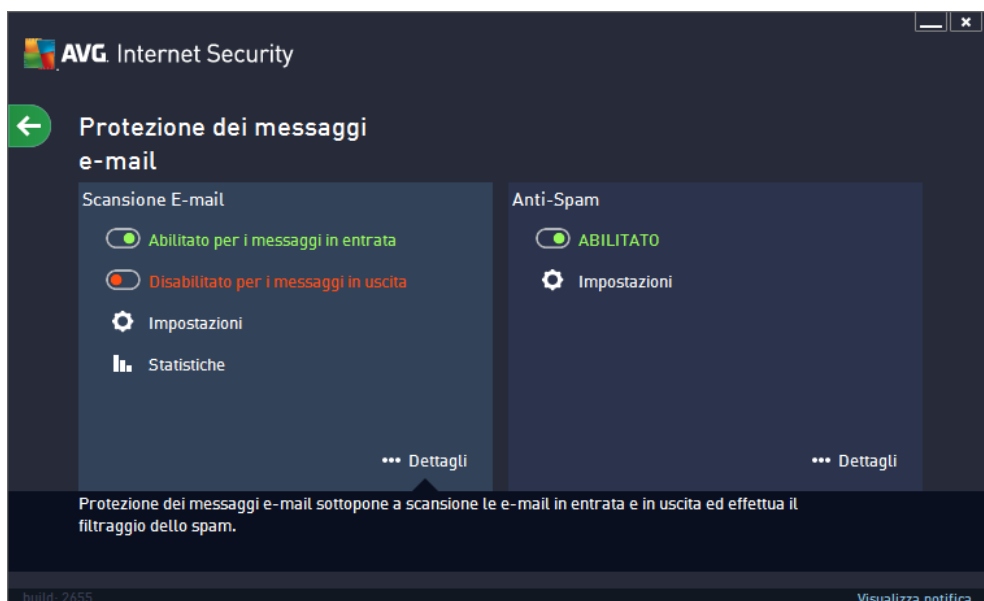
: usare la freccia verde nella parte superiore sinistra della finestra di dialogo per tornare all' interfaccia utente principale con la panoramica dei componenti.

Nella sezione Identity Protection è possibile trovare anche il pulsante ***Visualizza e imposta il mio account Identity Alert***. Utilizzare questo pulsante per essere reindirizzati alla pagina Web dedicata a Identity Alert in cui è necessario attivare il servizio.

6.4. E-mail

Il componente ***Protezione dei messaggi e-mail*** include due servizi di protezione: ***Scansione E-mail*** e ***Anti-Spam***.

- ***Scansione E-mail***: una delle origini più comuni di virus e trojan è la posta elettronica. Phishing e spam rendono l'e-mail una fonte di rischio ancora più grande. Gli account e-mail gratuiti sono quelli che presentano più probabilità di ricevere questo tipo di messaggi dannosi *(poiché raramente impiegano una tecnologia antispam)* e gli utenti domestici si affidano moltissimo a questo tipo di e-mail. Inoltre, gli utenti domestici aumentano l'esposizione ad attacchi tramite e-mail poiché navigano spesso in siti sconosciuti e compilano moduli in linea con dati personali *(ad esempio l'indirizzo e-mail)*. Di solito le società utilizzano account aziendali, filtri antispam e altri accorgimenti per ridurre il rischio. Il componente Protezione dei messaggi e-mail è responsabile della scansione di tutti i messaggi e-mail inviati o ricevuti. Ogni volta che viene rilevato un virus in un'e-mail, questo viene immediatamente spostato in Quarantena virus. Il componente, inoltre, può filtrare alcuni tipi di allegati e-mail e aggiungere un testo di certificazione ai messaggi non infetti. ***Il componente Scansione E-mail non è destinato alle piattaforme server.***

- ***Anti-Spam*** consente di controllare tutti i messaggi e-mail in arrivo e di contrassegnare quelli indesiderati come spam *(il termine "spam" indica messaggi di posta indesiderati, per lo più pubblicità di prodotti o servizi, inviate in massa e simultaneamente a un enorme numero di indirizzi di posta elettronica, che intasano le cassette postali dei destinatari. Lo spam non rientra nella categoria dei legittimi messaggi e-mail commerciali per i quali i consumatori hanno fornito il consenso.)*. Anti-Spam può modificare l'oggetto dell'e-mail *(identificata come spam)* aggiungendo una stringa di testo speciale. Sarà quindi possibile filtrare rapidamente i messaggi e-mail nel client e-mail. Il componente Anti-Spam utilizza diversi metodi di analisi per elaborare ciascun messaggio e-mail, offrendo il massimo livello di protezione possibile contro i messaggi e-mail indesiderati. Anti-Spam utilizza un database aggiornato regolarmente per il rilevamento dello spam. È inoltre possibile utilizzare i server RBL *(database pubblici di indirizzi e-mail di spammer noti)* e aggiungere manualmente indirizzi e-mail alla whitelist *(indirizzi da non contrassegnare mai come spam)* e alla blacklist *(indirizzi da contrassegnare sempre come spam)*.

Comandi della finestra di dialogo

Per passare da una sezione all'altra della finestra di dialogo, è possibile fare clic in qualsiasi punto del rispettivo pannello di servizio. Il pannello viene evidenziato in una tonalità di blu più chiara. In entrambe le sezioni della finestra di dialogo è possibile trovare i seguenti controlli. La funzionalità è la stessa, indipendentemente dal servizio di protezione a cui appartengono *(Scansione E-mail o Anti-Spam)*:

Attivato / Disattivato : questo pulsante è simile a un semaforo, sia nell'aspetto che nella funzionalità. Fare clic per passare da una posizione all'altra. Il colore verde significa ***Attivato***, ovvero indica che il servizio di protezione è attivo e completamente funzionante. Il colore rosso rappresenta lo stato ***Disattivato*** , ovvero indica che il servizio è disabilitato. A meno che non sussista un motivo valido per disattivare il servizio, si consiglia di mantenere le impostazioni predefinite per tutte le configurazioni di protezione. Le impostazioni predefinite assicurano prestazioni ottimali dell'applicazione e massima protezione. Se per qualche ragione si desidera disattivare il servizio, per mettere in guardia dai possibili rischi verrà subito visualizzato il simbolo rosso di ***Avviso*** e l'utente verrà informato che la protezione non è completa. ***Tenere presente che è necessario riattivare il servizio il prima possibile.***

Nella sezione Scansione dei messaggi e-mail è possibile visualizzare due dei pulsanti "semaforo". In questo modo è possibile specificare separatamente se si desidera che Scansione E-mail controlli i messaggi in entrata, in uscita o entrambi. Per impostazione predefinita, la scansione è attivata per i messaggi in entrata, mentre è disattivata per quelli in uscita in cui il rischio di infezione è minimo.

Impostazioni: facendo clic su questo pulsante si viene reindirizzati all'area delle impostazioni avanzate. Verrà aperta la relativa finestra di dialogo e sarà possibile configurare il servizio selezionato, ovvero Scansione E-mail o Anti-Spam. Nell'area delle impostazioni avanzate è possibile modificare la configurazione di ogni servizio di protezione tramite **AVG Internet Security 2013**, tuttavia le eventuali modifiche sono consigliate ai soli utenti esperti.

Statistiche : facendo clic su questo pulsante si viene reindirizzati alla pagina dedicata nel sito web di AVG (http://www.avg.com/). In tale pagina è disponibile una panoramica statistica dettagliata di tutte le attività di **AVG Internet Security 2013** eseguite sul computer in uno specifico periodo di tempo e in totale.

Dettagli: facendo clic su questo pulsante, nella parte inferiore della finestra di dialogo verrà visualizzata una breve descrizione del servizio evidenziato.

: usare la freccia verde nella parte superiore sinistra della finestra di dialogo per tornare all' interfaccia utente principale con la panoramica dei componenti.

6.5. Firewall

Il componente ***Firewall*** è un sistema che impone un criterio di controllo dell'accesso tra due o più reti bloccando o consentendo il traffico. Inoltre contiene un insieme di regole che proteggono la rete interna da attacchi *esterni (normalmente da Internet)* e controlla tutte le comunicazioni su ogni singola porta di rete. La comunicazione viene valutata in base alle regole definite, quindi viene eventualmente consentita o impedita. Se il componente Firewall rileva tentativi di intrusione, li blocca immediatamente e non consente all'intruso di accedere al PC. Il componente Firewall viene configurato per consentire o negare le comunicazioni interne/esterne *(in entrambe le direzioni, entrata o uscita)* tramite le porte definite e per le applicazioni software definite. Ad esempio, potrebbe essere configurato per consentire il solo flusso dei dati Web in entrata e in uscita tramite Microsoft Internet Explorer. Qualsiasi tentativo di trasmettere i dati Web tramite un altro browser viene quindi bloccato. Il componente Firewall impedisce l'invio non autorizzato delle informazioni di identificazione personale contenute nel computer. Controlla inoltre il modo in cui il computer scambia i dati con altri computer in Internet o nella rete locale. All'interno di un'organizzazione il componente Firewall protegge anche i singoli computer da attacchi lanciati da utenti interni ai computer nella rete.

In **AVG Internet Security 2013**, il componente ***Firewall*** controlla tutto il traffico in ogni porta di rete del computer. In base alle regole definite, il componente Firewall valuta le applicazioni in esecuzione sul computer *(che vogliono eseguire la connessione alla rete locale o a Internet)* oppure le applicazioni che dall'esterno tentano di connettersi al PC dell'utente. Per ciascuna di queste applicazioni, il componente Firewall consente o impedisce la comunicazione sulle porte di rete. Per impostazione predefinita, se l'applicazione è sconosciuta *(ovvero non dispone di regole Firewall definite)*, verrà richiesto di consentire o bloccare il tentativo di comunicazione.

AVG Firewall non è destinato alla protezione delle piattaforme server.

Consiglio: *in genere non è consigliabile utilizzare più di un firewall su un singolo computer. Il livello di protezione del computer non è maggiore se si installano più firewall. È più probabile che si verifichino conflitti tra queste applicazioni. Si consiglia, pertanto, di utilizzare un solo firewall nel computer e di disattivare gli altri, eliminando così il rischio di possibili conflitti e problemi correlati.*

Modalità Firewall disponibili

Il componente Firewall consente di definire le regole di protezione specifiche a seconda che si tratti di un computer presente in un dominio, di un computer autonomo o perfino di un notebook. Ogni opzione richiede un livello diverso di protezione e i livelli sono coperti dalle rispettive modalità. In breve, una modalità Firewall è una specifica configurazione del componente Firewall ed è possibile utilizzare diverse di queste configurazioni predefinite.

- ***Automatica***: in questa modalità il componente Firewall gestisce tutto il traffico di rete automaticamente. Non verrà richiesto l'intervento dell'utente. Il componente Firewall consentirà la connessione a tutte le applicazioni note e contemporaneamente verrà creata una regola che indica che tale applicazione può connettersi sempre in futuro. Per altre applicazioni, Firewall deciderà se consentire o bloccare la connessione in base al comportamento dell'applicazione. Tuttavia, in questa situazione non verrà creata alcuna regola e l'applicazione verrà controllata nuovamente quando tenta di connettersi. La modalità automatica è abbastanza discreta ed è consigliata per la maggior parte degli utenti.

- ***Interattiva***: questa modalità è utile se si desidera controllare completamente tutto il traffico di rete in ingresso e in uscita dal computer. Il componente Firewall monitorerà il traffico e notificherà all'utente ogni tentativo di comunicazione o trasferimento dati, permettendo all'utente di consentire o bloccare i tentativi come desidera. Opzione consigliata solo per utenti esperti.

- ***Blocca l'accesso a Internet***: la connessione a Internet viene bloccata completamente, è impossibile accedere a Internet e nessuno può accedere al computer dall'esterno. Solo per uso eccezionale e per breve tempo.

- ***Disattiva la protezione Firewall***: la disattivazione del Firewall consentirà tutto il traffico di rete in entrata e in uscita dal computer. Di conseguenza, il computer sarà esposto agli attacchi di hacker. Valutare sempre questa opzione con attenzione.

Tenere presente che una modalità automatica specifica è disponibile anche nel Firewall. Questa modalità viene attivata in modo invisibile se i componenti Protezione del computer o Identity Protection vengono disattivati rendendo il computer più vulnerabile. In tali casi, il componente Firewall consentirà automaticamente solo le applicazioni note e assolutamente sicure. Per tutti gli altri casi, verrà richiesto all'utente come procedere. Ciò consente di ovviare alla disattivazione dei componenti di protezione e di mantenere il computer protetto.

Comandi della finestra di dialogo

La finestra di dialogo fornisce una panoramica delle informazioni di base sullo stato del componente Firewall:

- ***Modalità Firewall***: fornisce informazioni sulla modalità Firewall attualmente selezionata. Utilizzare il pulsante ***Modifica*** accanto all'informazione fornita per passare all'interfaccia Impostazioni del Firewall se si desidera modificare la modalità corrente con un'altra *(per descrizioni e consigli sull'utilizzo dei profili Firewall vedere il paragrafo precedente)*.

- ***Condivisione file e stampanti***: indica se la condivisione di file e stampanti *(in entrambe le direzioni)* al momento è disponibile. Condivisione di file e stampanti significa condividere qualsiasi file o cartella contrassegnato come "Condiviso" in Windows, in unità disco comuni, stampanti, scanner e dispositivi simili. È preferibile condividere tali elementi solo all'interno di reti considerate sicure *(ad esempio a casa, in ufficio o a scuola)*. Tuttavia, se si è connessi a una rete pubblica *(ad esempio, al Wi-Fi dell'aeroporto o di un Internet Point)*, è consigliabile non condividere nulla.

- ***Connesso a***: fornisce informazioni sul nome della rete a cui si è attualmente connessi. Con Windows XP, il nome della rete corrisponde alla denominazione scelta per la rete specifica durante la prima connessione. Con Windows Vista e versioni successive, il nome della rete viene ricavato automaticamente dal Centro connessioni di rete e condivisione.

Nella finestra di dialogo sono disponibili i seguenti comandi:

Modifica: questo pulsante consente di modificare lo stato di un relativo parametro. Per ulteriori dettagli sul processo di modifica vedere la descrizione dei parametri specifici nel paragrafo sopra.

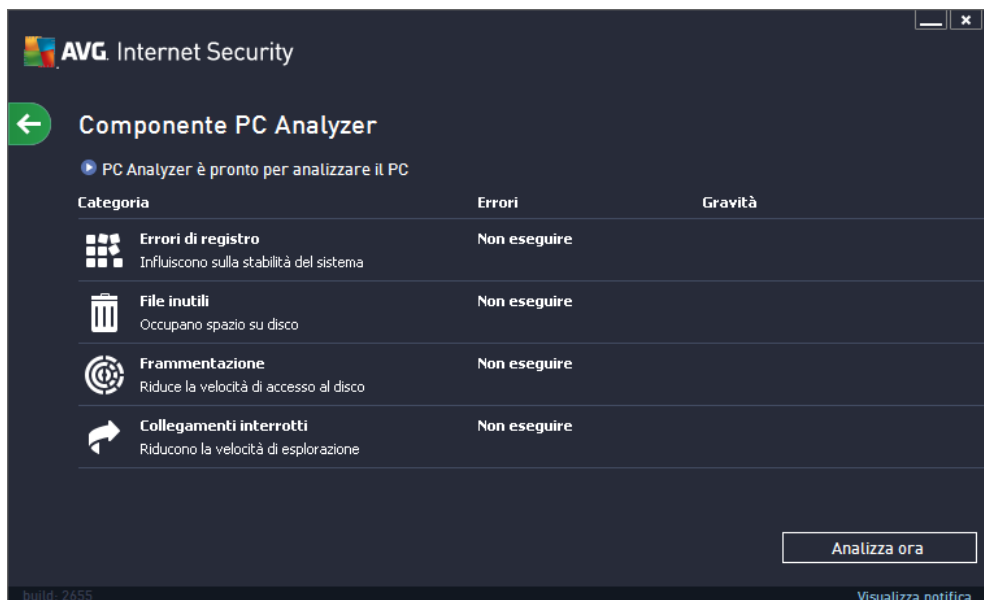
Impostazioni: fare clic sul pulsante per essere reindirizzati all'interfaccia Impostazioni del Firewall in cui è possibile modificare tutte le configurazioni del Firewall. Qualunque configurazione deve essere eseguita solo da utenti esperti!

Reimposta su predefinito: selezionare questo pulsante per sovrascrivere la configurazione corrente del Firewall e ripristinare la configurazione predefinita basata sul rilevamento automatico.

Dettagli: facendo clic su questo pulsante, nella parte inferiore della finestra di dialogo verrà visualizzata una breve descrizione del servizio evidenziato.

: usare la freccia verde nella parte superiore sinistra della finestra di dialogo per tornare all' interfaccia utente principale con la panoramica dei componenti.

6.6. PC Analyzer

Il componente ***PC Analyzer*** esamina il computer per rilevare problemi di sistema e fornisce una panoramica dettagliata di ciò che potrebbe ridurre le prestazioni globali del computer:

Nell'interfaccia utente del componente è possibile visualizzare un grafico diviso in quattro righe relative alle seguenti categorie: errori di registro, file inutili, frammentazione e collegamenti interrotti.

- ***Errori di registro*** fornisce il numero di errori nel Registro di Windows. Poiché la correzione del Registro richiede particolare esperienza, si consiglia di non correggere il Registro personalmente.

- ***File inutili*** fornisce il numero di file che sono molto probabilmente superflui. In genere si tratta di file temporanei di vario tipo e dei file presenti nel Cestino.

- ***Frammentazione*** consente di calcolare la percentuale di disco rigido frammentata, ovvero utilizzata per molto tempo per cui al momento i file si trovano sparsi in diverse parti del disco fisico. È possibile utilizzare strumenti per la deframmentazione per correggere questa situazione.

- ***Collegamenti interrotti*** indica all'utente collegamenti non più funzionanti, che conducono a posizioni inesistenti e così via.

Per avviare l'analisi del sistema, selezionare il pulsante ***Analizza ora***. Sarà quindi possibile visualizzare l'avanzamento dell'analisi e i relativi risultati direttamente nel grafico. La panoramica dei risultati fornisce il numero di problemi del sistema rilevati (***Errori***) divisi in base alle categorie controllate. I risultati dell'analisi verranno inoltre visualizzati graficamente nella colonna ***Gravità***.

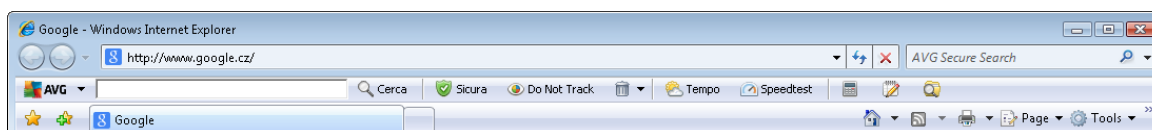
Pulsanti di controllo

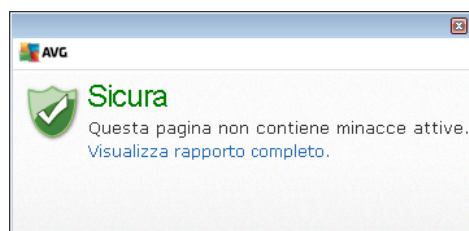
- ***Analizza ora*** (*visualizzato prima dell'avvio dell'analisi*): selezionare questo pulsante per avviare immediatamente l'analisi del computer

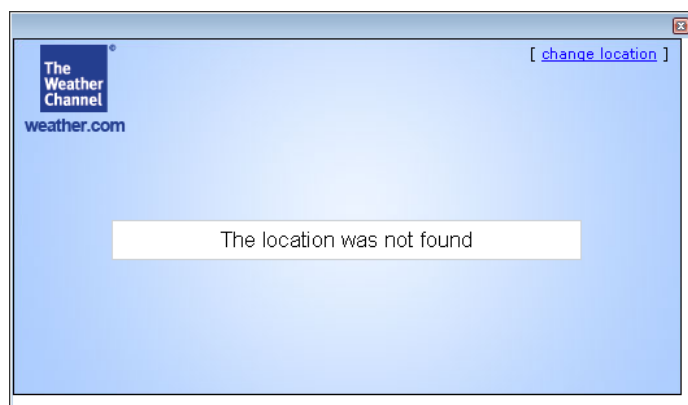
- ***Correggi ora*** (*visualizzato al completamento dell'analisi*): selezionare il pulsante per visualizzare il sito Web di AVG (http://www.avg.com/) alla pagina contenente informazioni dettagliate e aggiornate correlate al componente ***PC Analyzer***

- ***Annulla***: selezionare il pulsante per arrestare l'analisi in corso o per tornare alla finestra di dialogo principale di AVG predefinita (*panoramica dei componenti*) al completamento dell'analisi

7. AVG Security Toolbar

AVG Security Toolbar è uno strumento che funziona insieme al servizio LinkScanner Surf-Shield per assicurare la protezione massima durante l'esplorazione di Internet. All'interno di **AVG Internet Security 2013**, l'installazione di ***AVG Security Toolbar*** è opzionale; durante il processo di installazione viene richiesto se installare o meno il componente. ***AVG Security Toolbar*** è disponibile direttamente nel browser Internet. Al momento, i browser Internet supportati sono Internet Explorer (*versione 6.0 e successive*) e/o Mozilla Firefox (*versione 3.0 e successive*). Non sono supportati altri browser *(se si utilizza un browser Internet alternativo, ad esempio Avant Browser, è possibile che si verifichino comportamenti inattesi).*

AVG Security Toolbar si compone dei seguenti elementi:

- ***Logo AVG*** con il menu a discesa:
    - ***Usa AVG Secure Search***: consente di effettuare ricerche direttamente da ***AVG Security Toolbar*** utilizzando il motore ***AVG Secure Search***.
    - ***Livello di minacce corrente***: consente di aprire la pagina Web di Virus Lab contenente la visualizzazione grafica del livello di minacce corrente sul Web.
    - ***AVG Threat Labs***: apre il sito Web specifico di ***AVG Threat Lab*** *(all'indirizzo http://www.avgthreatlabs.com)*, dove è possibile ottenere informazioni relative alla sicurezza di vari siti Web e all'attuale livello di rischio in linea.
    - ***Guida di AVG Security Toolbar***: apre la Guida in linea che tratta tutte le funzionalità di ***AVG Security Toolbar***.
    - ***Invia commenti sul prodotto***: apre una pagina Web che contiene un modulo utilizzabile per inviare commenti circa ***AVG Security Toolbar***.
    - ***Disinstalla AVG Security Toolbar***: apre una pagina Web contenente una descrizione dettagliata su come disattivare ***AVG Security Toolbar*** in ognuno dei browser Web supportati.
    - ***Informazioni su...***: apre una nuova finestra contenente informazioni sulla versione installata di ***AVG Security Toolbar***.
- ***Campo di ricerca***: consente di effettuare ricerche in Internet utilizzando ***AVG Security Toolbar*** per essere certi che tutti i risultati visualizzati siano sicuri al 100%. Immettere una parola chiave o una frase nel campo di ricerca, quindi fare clic sul pulsante ***Cerca*** *(o premere Invio).*
- ***Sicurezza sito***: questo pulsante consente di aprire una nuova finestra di dialogo con le informazioni sull'attuale livello di rischio (*Attualmente sicuro*) della pagina che si sta visitando. Questa breve panoramica può essere espansa e visualizzata con informazioni complete su tutte le attività di protezione relative alla pagina nella finestra del browser (*Visualizza rapporto completo*):

- ***Elimina***: tramite l'icona del cestino è possibile visualizzare un menu a discesa che consente di scegliere se eliminare le informazioni su esplorazione, download e moduli in linea oppure eliminare l'intera cronologia ricerche.

- ***Meteo***: questo pulsante apre una nuova finestra di dialogo contenente le informazioni sul meteo attuale nella località di residenza e le previsioni per i due giorni successivi. Queste informazioni vengono aggiornate regolarmente ogni 3-6 ore. Nella finestra di dialogo è possibile cambiare la località desiderata manualmente e specificare se visualizzare le informazioni relative alla temperatura in gradi Celsius o Fahrenheit.

- ***Facebook***: questo pulsante consente di effettuare la connessione al social network Facebook direttamente da ***AVG Security Toolbar***

- ***Speedtest***: questo pulsante reindirizza a un'applicazione in linea che consente di verificare la qualità della connessione a Internet *(ping)* e la velocità di download e di caricamento.

- Pulsanti di scelta rapida per l'accesso rapido alle seguenti applicazioni: ***Calcolatrice***, ***Blocco note***, ***Esplora risorse***.

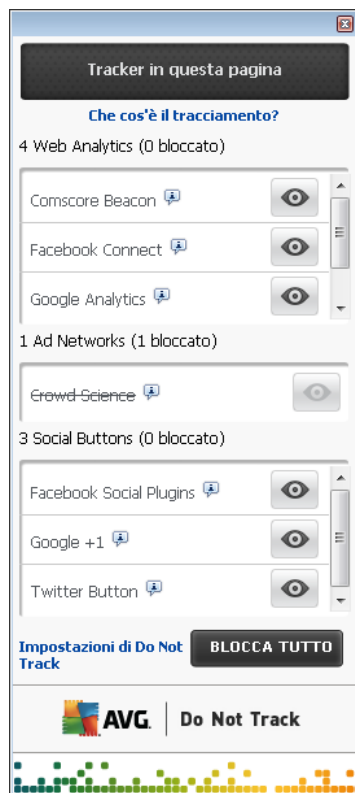
8. AVG Do Not Track

AVG Do Not Track consente di individuare i siti Web che raccolgono informazioni sulle attività in linea dell'utente. Un'icona nel browser consente di visualizzare i siti Web e gli inserzionisti che raccolgono informazioni sull'attività dell'utente, che può scegliere di consentirli o impedirli.

- ***AVG Do Not Track*** fornisce informazioni aggiuntive sull'informativa sulla privacy di ciascun servizio, oltre a un collegamento che consente di revocare l'adesione al servizio (se disponibile).
- ***AVG Do Not Track*** utilizza inoltre il protocollo W3C DNT per segnalare automaticamente ai siti che l'utente desidera impedire il tracciamento. Questa notifica è abilitata per impostazione predefinita, ma può essere modificata in qualsiasi momento.
- ***AVG Do Not Track*** viene fornito in base a questi termini e condizioni.
- ***AVG Do Not Track è abilitato per impostazione predefinita, ma può essere disabilitato in qualsiasi momento.*** Per le istruzioni dettagliate, vedere l'articolo nella sezione delle domande frequenti Disattivazione della funzionalità AVG Do Not Track.
- Per ulteriori informazioni su ***AVG Do Not Track***, visitare il sito Web di AVG.

La funzionalità ***AVG Do Not Track*** è attualmente supportata nei browser Mozilla Firefox, Chrome e Internet Explorer. *In Internet Explorer l'icona di AVG Do Not Track si trova sul lato destro della barra dei comandi. In caso di problemi di visualizzazione dell'icona di AVG Do Not Track con le impostazioni predefinite del browser, assicurarsi che la barra dei comandi sia stata attivata. Se non è comunque possibile visualizzare l'icona, trascinare la barra dei comandi a sinistra per visualizzare tutte le icone e i pulsanti disponibili sulla barra degli strumenti.*

8.1. Interfaccia di AVG Do Not Track

Mentre l'utente è in linea, ***AVG Do Not Track*** lo avvisa non appena viene rilevata una qualsiasi attività di raccolta delle informazioni. Verrà visualizzata la finestra di dialogo seguente:

Tutti i servizi di raccolta delle informazioni rilevati vengono elencati per nome nel riepilogo ***Tracker in questa pagina***. Esistono tre tipi di attività di raccolta delle informazioni riconosciuti da ***AVG Do Not Track***:

- ***Web Analytics*** *(consentiti per impostazione predefinita):* servizi utilizzati per l'ottimizzazione delle prestazioni e dell'esperienza nel relativo sito Web. Questa categoria include servizi come Google Analytics, Omniture o Yahoo Analytics. Si consiglia di non bloccare i servizi di Web Analytics, poiché il sito Web potrebbe non funzionare correttamente.

- ***Social button*** *(consentiti per impostazione predefinita):* elementi progettati per il miglioramento dell'esperienza nei social network. I social button sono i pulsanti che alcuni social network inseriscono in altri siti con l'intento di raccogliere informazioni sull'attività in linea degli utenti che eseguono l'accesso. Alcuni esempi di social button sono i plugin e i pulsanti di Facebook, Twitter e Google.

- ***Ad Network*** *(alcuni sono bloccati per impostazione predefinita):* servizi che raccolgono o condividono informazioni sull'attività in linea dell'utente in più siti, sia direttamente che indirettamente, al fine di offrire contenuti pubblicitari personalizzati, diversamente dalle inserzioni basate sul contenuto. I dettagli di tale processo vengono definiti nell'informativa sulla privacy disponibile nel sito di ciascuna Ad Network. Alcuni servizi Ad Network sono bloccati per impostazione predefinita.

Nota: *in base ai servizi eseguiti in background nel sito Web, alcune di queste sezioni potrebbero non essere visualizzate nella finestra di AVG Do Not Track.*

Nella finestra di dialogo sono inoltre disponibili due collegamenti:

- ***Che cos'è il tracciamento?*** – Facendo clic su questo collegamento nella parte superiore della finestra di dialogo si viene reindirizzati a una pagina Web dedicata che fornisce informazioni dettagliate sui principi del rilevamento e una descrizione dei diversi tipi di rilevamento.

- ***Impostazioni*** – Facendo clic su questo collegamento nella parte superiore della finestra di dialogo si viene reindirizzati a una pagina Web dedicata in cui è possibile configurare vari parametri di ***AVG Do Not Track***. *Per informazioni dettagliate, vedere il capitolo* *Impostazioni di AVG Do Not Track*.

8.2. Informazioni sui processi di rilevamento

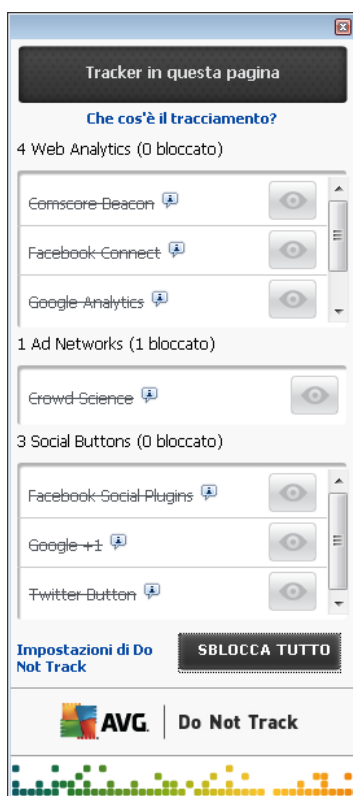
L'elenco dei servizi di raccolta delle informazioni individuati fornisce solo il nome di ogni servizio. Per decidere in modo efficace se bloccare o consentire un determinato servizio, potrebbero essere necessarie ulteriori informazioni. Spostare il mouse sulla voce dell'elenco desiderata. Viene visualizzato un riquadro con informazioni dettagliate sul servizio. In questo modo, è possibile sapere se il servizio raccoglie i dati personali, o altre informazioni disponibili, e se i dati raccolti vengono condivisi con terze parti e archiviati per essere utilizzati in seguito.

Nella parte inferiore del riquadro informativo è disponibile il collegamento ***Informativa sulla privacy***, che reindirizza al sito Web dedicato all'informativa sulla privacy del corrispondente servizio rilevato.

8.3. Blocco dei processi di rilevamento

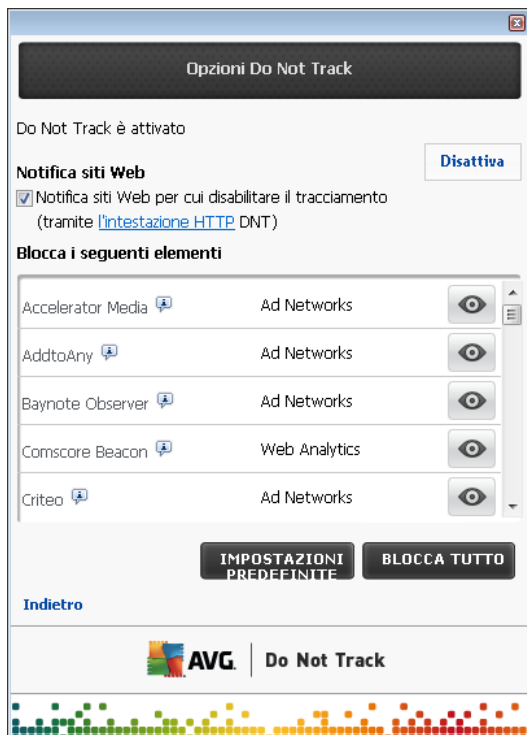
Gli elenchi Social button, Ad Network e Web Analytics consentono di controllare quali servizi devono essere bloccati. È possibile procedere in due modi:

- ***Blocca tutto***: fare clic su questo pulsante nella parte inferiore della finestra di dialogo per impedire tutte le attività di raccolta delle informazioni. *Nota: questa azione potrebbe compromettere il funzionamento della pagina Web dove il servizio è in esecuzione.*

- Se non si desidera bloccare contemporaneamente tutti i servizi rilevati, è possibile specificare per ogni servizio se deve essere consentito o bloccato. È possibile consentire l'esecuzione di alcuni dei sistemi rilevati *(ad esempio, Web Analytics)*, che utilizzano i dati raccolti per l'ottimizzazione del sito Web, favorendo il miglioramento dell'ambiente Internet per tutti gli utenti. Tuttavia, è possibile bloccare contemporaneamente le attività di raccolta delle informazioni da parte di tutti i processi classificati come Ad Network. È sufficiente fare clic sull'icona accanto al servizio per bloccare la raccolta delle informazioni *(il nome del processo verrà visualizzato barrato)* o consentirla nuovamente.

8.4. Impostazioni di AVG Do Not Track

Nella finestra di dialogo ***AVG Do Not Track*** è presente una sola opzione di configurazione: nella parte inferiore della finestra è possibile visualizzare la casella di controllo ***Avvisa quando vengono rilevati tracker attivi***. Per impostazione predefinita, questo elemento è disattivato. Selezionare questa casella di controllo per ricevere una notifica ogni volta che si accede a una pagina Web contenente un nuovo servizio di raccolta delle informazioni che non è ancora stato bloccato. Quando è selezionata, se nella pagina che si sta visitando viene individuato un nuovo servizio di raccolta

delle informazioni, ***AVG Do Not Track*** visualizza la finestra di dialogo di notifica. In caso contrario, la presenza del nuovo servizio rilevato verrà segnalata solo dal ***cambiamento di colore*** (da verde a giallo) dell'*icona di AVG Do Not Track*, disponibile sulla barra dei comandi del browser.

Nella parte inferiore della finestra di ***AVG Do Not Track*** è comunque disponibile il collegamento ***Impostazioni***. Facendo clic su questo collegamento si accede a una pagina Web in cui è possibile specificare in modo dettagliato le ***opzioni di AVG Do Not Track***:

Invia avviso

- ***Posizione della notifica*** *(per impostazione predefinita, nell'angolo superiore destro)* : aprire il menu a discesa per specificare la posizione desiderata per la finestra di ***AVG Do Not Track*** sullo schermo.

- ***Visualizza notifica per*** *(per impostazione predefinita, il valore è 10)* : in questo campo è possibile specificare l'intervallo di tempo *(in secondi)* per cui la notifica di ***AVG Do Not Track*** deve essere visualizzata. È possibile specificare un valore compreso tra 0 e 60 secondi*. Se il valore specificato è 0, la notifica non viene visualizzata.*

- ***Avvisa quando vengono rilevati tracker attivi*** *(deselezionata per impostazione predefinita)*: selezionare questa casella di controllo per ricevere una notifica ogni volta che si accede a una pagina Web contenente un nuovo servizio di rilevamento che non è ancora stato bloccato. Quando è selezionata, se nella pagina che si sta visitando viene individuato un nuovo servizio di raccolta delle informazioni, ***AVG Do Not Track*** visualizza la finestra di dialogo di notifica. In caso contrario, la presenza del nuovo servizio rilevato verrà segnalata solo dal ***cambiamento di colore*** (da verde a giallo) dell'*icona di AVG Do Not Track, disponibile sulla barra dei comandi del browser.*

- ***Notifica siti Web per cui disabilitare il tracciamento*** *(selezionata per impostazione predefinita)* : lasciare selezionata questa opzione se si desidera che ***AVG Do Not Track*** informi il provider di un servizio di raccolta delle informazioni che si desidera impedire il tracciamento.

Blocca i seguenti elementi

In questa sezione è possibile visualizzare un riquadro con l'elenco dei servizi di raccolta dati noti classificabili come Ad Network. Per impostazione predefinita, ***AVG Do Not Track*** blocca automaticamente alcuni Ad Network ed è possibile scegliere se bloccare anche i restanti o mantenerli abilitati. A tale scopo, fare clic sul pulsante ***Blocca tutto*** sotto l'elenco.

Pulsanti di controllo

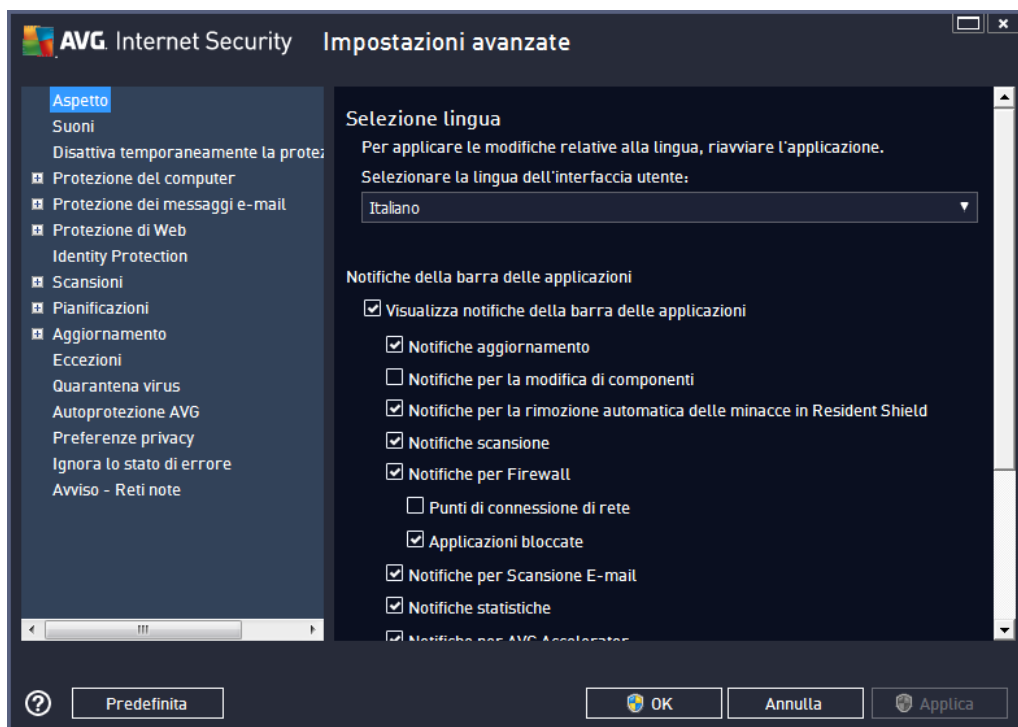
Nella pagina ***Opzioni di AVG Do Not Track*** sono disponibili i seguenti pulsanti di opzione:

- ***Blocca tutto***: selezionare per bloccare contemporaneamente tutti i servizi elencati nella casella precedente e classificati come Ad Network.
- ***Consenti tutto***: selezionare per sbloccare contemporaneamente tutti i servizi bloccati elencati nella casella precedente e classificati come Ad Network.
- ***Impostazioni predefinite***: selezionare per eliminare tutte le impostazioni personalizzate e ripristinare la configurazione predefinita.
- ***Salva***: fare clic per applicare e salvare la configurazione specificata.
- ***Annulla***: fare clic per annullare tutte le impostazioni precedentemente specificate.

9. Impostazioni AVG avanzate

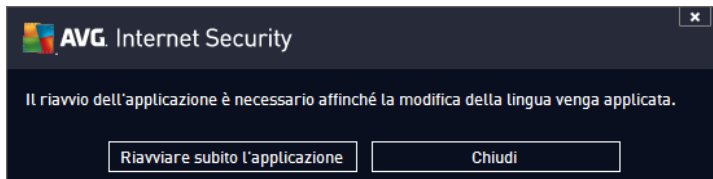
Le opzioni di configurazione avanzata di **AVG Internet Security 2013** sono disponibili in una nuova finestra denominata ***Impostazioni AVG avanzate***. La finestra è suddivisa in due sezioni: la parte sinistra fornisce una struttura di esplorazione per accedere alle opzioni di configurazione del programma. Selezionare il componente di cui si desidera modificare la configurazione (*o una parte specifica*) per aprire la finestra di dialogo di modifica nella sezione destra della finestra.

9.1. Aspetto

La prima voce della struttura di esplorazione, ***Aspetto***, fa riferimento alle impostazioni generali dell' interfaccia utente di **AVG Internet Security 2013** e fornisce alcune opzioni di base relative al comportamento dell'applicazione:

Selezione lingua

Nella sezione ***Selezione lingua*** è possibile scegliere la lingua desiderata dal menu a discesa. La lingua selezionata verrà quindi utilizzata per l'intera interfaccia utente di **AVG Internet Security 2013**. Nel menu a discesa sono presenti solo le lingue selezionate in precedenza per essere installate durante il processo di installazione e l'inglese (*sempre installato automaticamente per impostazione predefinita*). Per completare l'impostazione di **AVG Internet Security 2013** su un'altra lingua è necessario riavviare l'applicazione. Procedere come segue:

- Nel menu a discesa, selezionare la lingua desiderata per l'applicazione
- Confermare la selezione facendo clic sul pulsante ***Applica*** *(angolo inferiore destro della finestra di dialogo)*

- Fare clic sul pulsante ***OK*** per confermare
- Viene visualizzata una nuova finestra di dialogo che comunica che per modificare la lingua dell'applicazione è necessario riavviare **AVG Internet Security 2013**
- Fare clic su pulsante ***Riavviare subito l'applicazione*** per confermare il riavvio del programma e attendere alcuni istanti l'applicazione della modifica della lingua:

Notifiche della barra delle applicazioni

In questa sezione è possibile eliminare la visualizzazione delle notifiche della barra delle applicazioni sullo stato dell'applicazione **AVG Internet Security 2013**. Per impostazione predefinita, le notifiche della barra delle applicazioni vengono visualizzate. Si consiglia di mantenere questa impostazione. Le notifiche di sistema comunicano, ad esempio, l'avvio del processo di scansione o aggiornamento o una modifica dello stato di un componente di **AVG Internet Security 2013**. Questi avvisi devono essere tenuti nella dovuta considerazione.

Tuttavia, se per qualche ragione non si desidera visualizzare tali notifiche o si desidera visualizzarne solo alcune *(correlate a un componente di AVG Internet Security 2013 specifico)*, è possibile definire e specificare le proprie preferenze selezionando/deselezionando le seguenti opzioni:

- ***Visualizza notifiche della barra delle applicazioni*** *(attivata per impostazione predefinita)* : per impostazione predefinita, tutte le notifiche vengono visualizzate. Deselezionare questa voce per disattivare completamente la visualizzazione delle notifiche di sistema. Quando è attivata, è possibile selezionare inoltre le notifiche specifiche da visualizzare:
  - ***Notifiche aggiornamento*** *(attivata per impostazione predefinita)*: consente di decidere se visualizzare le informazioni relative **AVG Internet Security 2013** all'avvio, all'avanzamento e alla finalizzazione del processo di aggiornamento.
  - ***Notifiche per la modifica dei componenti*** *(disattivata per impostazione predefinita)* : consente di decidere se visualizzare le informazioni relative allo stato di attività/ inattività del componente o a un suo eventuale problema. Quando viene riportato lo stato di errore di un componente, questa opzione equivale alla funzione informativa dell'icona della barra delle applicazioni per indicare un problema di un componente di **AVG Internet Security 2013**.
  - ***Notifiche per la rimozione automatica delle minacce in Resident Shield*** *(attivata per impostazione predefinita)*: consente di decidere se visualizzare o meno le informazioni relative ai processi di salvataggio, copia e apertura dei file (*questa configurazione viene visualizzata solo se l'opzione Correzione automatica di Resident Shield è attiva*).
  - ***Notifiche scansione*** *(attivata per impostazione predefinita)*: consente di decidere se visualizzare le informazioni relative all'avvio automatico, all'avanzamento e ai risultati

della scansione pianificata.

- ***Visualizza notifiche della barra delle applicazioni correlate a Firewall*** *(attivata per impostazione predefinita)*: consente di decidere se visualizzare le informazioni relative ai processi e allo stato del componente Firewall, quali avvisi di attivazione/ disattivazione del componente, possibile blocco del traffico e così via. Questa voce fornisce altre due opzioni di selezione specifiche *(per la spiegazione dettagliata di ciascuna di esse consultare il capitolo Firewall di questo documento)*:

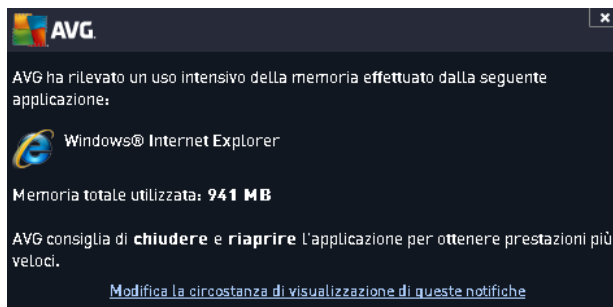
  - ***Visualizza notifiche per le modifiche dei profili*** *(attivata per impostazione predefinita)*: informa circa modifiche automatiche ai profili Firewall.

  - ***Visualizza notifiche per la nuova regola dell'applicazione creata*** *(disattivata per impostazione predefinita)*: informa l'utente circa la creazione automatica di regole Firewall per nuove applicazioni in base a un elenco di applicazioni sicure.

- ***Notifiche per Scansione E-mail*** *(attivata per impostazione predefinita)*: consente di decidere se visualizzare le informazioni relative alla scansione di tutti i messaggi e-mail in entrata e in uscita.

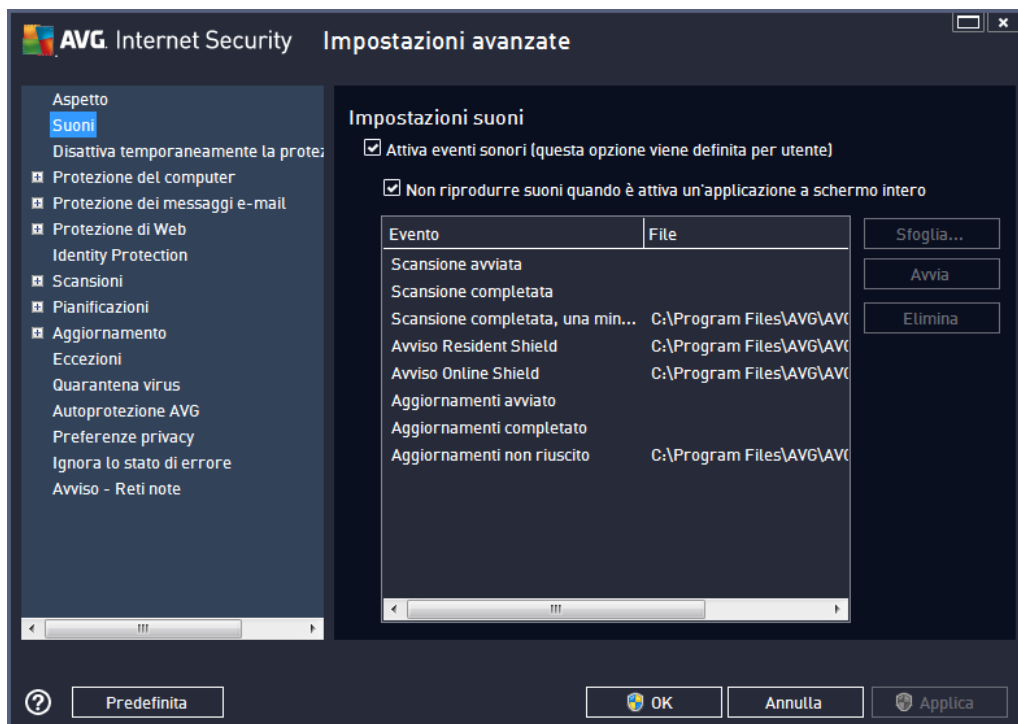
- ***Notifiche statistiche*** *(attivata per impostazione predefinita)* : mantenere l'opzione selezionata per consentire la visualizzazione di notifiche delle revisioni statistiche regolari nella barra delle applicazioni.

- ***Notifiche per AVG Accelerator*** *(attivata per impostazione predefinita)* : consente di decidere se visualizzare le informazioni relative alle attività di ***AVG Accelerator***. ***AVG Accelerator*** è un servizio che ottimizza la riproduzione dei video in linea e semplifica il download.

- ***Notifiche per AVG Advisor*** *(attivata per impostazione predefinita):*consente di decidere se visualizzare le informazioni relative alle attività di AVG Advisor nel pannello di scorrimento sulla barra delle applicazioni.

Modalità gioco

Questa funzione di AVG è stata progettata per le applicazioni a schermo intero, per le quali eventuali notifiche tramite fumetto di AVG (*visualizzate ad esempio all'avvio di una scansione pianificata*) potrebbero rappresentare una fonte di disturbo (*riducendole a icona o alterandone la grafica*). Per evitare questa situazione, mantenere selezionata la casella di controllo dell'opzione ***Abilita la modalità gioco quando viene eseguita un'applicazione a schermo intero*** (*impostazione predefinita*).

9.2. Suoni

Nella finestra di dialogo ***Suoni*** è possibile specificare se si desidera essere informati circa specifiche azioni di **AVG Internet Security 2013** tramite una notifica sonora:

Le impostazioni sono valide solo per l'account utente corrente, pertanto ogni utente del computer può disporre di impostazioni dei suoni personalizzate. Per consentire le notifiche sonore, mantenere l'opzione ***Attiva eventi sonori*** selezionata (*l'opzione è attivata per impostazione predefinita*) per attivare l'elenco di tutte le azioni correlate. Inoltre, è possibile selezionare l'opzione ***Non riprodurre suoni quando è attiva un'applicazione a schermo intero*** per eliminare le notifiche sonore quando potrebbero essere di disturbo *(vedere anche la sezione relativa alla modalità gioco del capitolo* *Impostazioni avanzate/Aspetto in questo documento)*.

Pulsanti di controllo

- ***Sfoglia***: dopo aver selezionato l'evento dall'elenco, utilizzare il pulsante ***Sfoglia*** per ricercare nel disco il file audio desiderato da assegnargli *(al momento sono supportati solo file *.wav).*

- ***Avvia***: per ascoltare il suono selezionato, evidenziare l'evento nell'elenco e fare clic sul pulsante ***Avvia***.

- ***Elimina***: utilizzare il pulsante ***Elimina*** per rimuovere il suono assegnato a uno specifico evento.

9.3. Disattiva temporaneamente la protezione di AVG

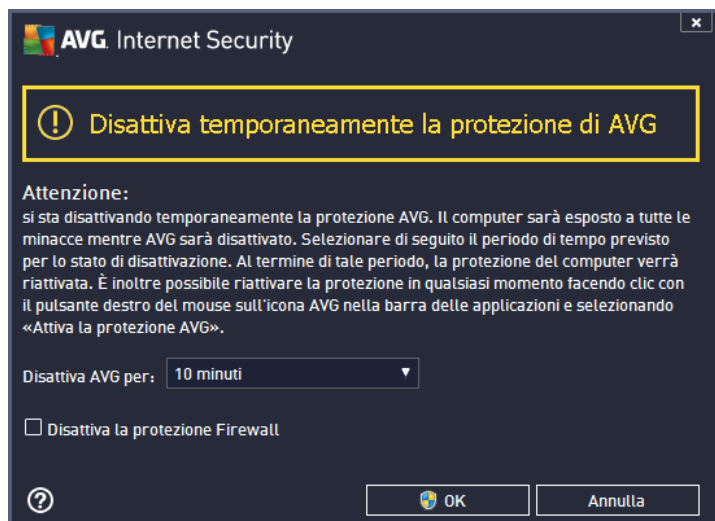
Nella finestra di dialogo ***Disabilitare temporaneamente la protezione di AVG*** è possibile disattivare l'intera protezione fornita da **AVG Internet Security 2013**.

Non utilizzare questa opzione se non è assolutamente necessario.

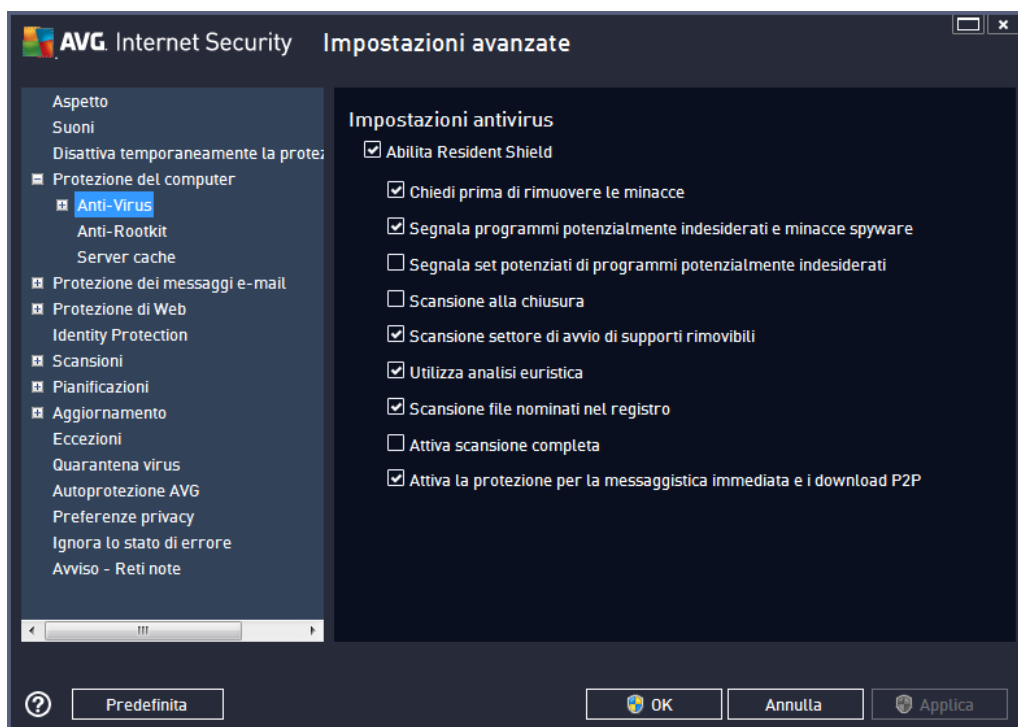
Nella maggior parte dei casi, ***non è necessario*** disattivare **AVG Internet Security 2013** prima di installare nuovi software o driver, neppure se il programma di installazione o la procedura guidata suggeriscono di chiudere tutti i programmi e le applicazioni in esecuzione per accertarsi che non si verifichino interruzioni indesiderate durante il processo di installazione. In caso di problemi durante l'installazione, provare innanzitutto a disattivare la protezione permanente (*Abilita Resident Shield*). Se fosse necessario disattivare temporaneamente **AVG Internet Security 2013**, lo si dovrà riattivare non appena possibile. Se si è connessi a Internet o a una rete mentre il software antivirus è disattivato, il computer sarà esposto a potenziali attacchi.

Come disattivare la protezione AVG

Selezionare la casella di controllo ***Disattiva temporaneamente la protezione di AVG*** e confermare la scelta facendo clic sul pulsante ***Applica***. Nella finestra di dialogo ***Disattiva temporaneamente la protezione di AVG*** aperta, specificare per quanto tempo si desidera disattivare **AVG Internet Security 2013**. Per impostazione predefinita, la protezione verrà disattivata per 10 minuti, tempo sufficiente per svolgere attività comuni quali l'installazione di un nuovo software e così via. È possibile impostare un periodo di tempo più lungo, tuttavia si consiglia di non utilizzare questa opzione se non è assolutamente necessario. Successivamente, tutti i componenti disattivati verranno riattivati automaticamente. È comunque possibile disattivare la protezione di AVG fino al

successivo riavvio del computer. Nella finestra di dialogo ***Disattiva temporaneamente la protezione di AVG*** è presente un'opzione distinta per disattivare il componente ***Firewall***. Per eseguire questa operazione, selezionare ***Disattiva la protezione Firewall***.

9.4. Protezione del computer

9.4.1. Anti-Virus

Anti-Virus e ***Resident Shield*** proteggono il computer in modo continuo da tutti i tipi noti di virus, spyware e malware in generale *(inclusi i cosiddetti malware dormienti e inattivi, ovvero i malware che sono stati scaricati ma non sono ancora stati attivati)*.

Nella finestra di dialogo ***Impostazioni di Resident Shield*** è possibile attivare o disattivare completamente la protezione permanente selezionando/deselezionando la voce ***Abilita Resident Shield*** (*questa opzione è attivata per impostazione predefinita*). Inoltre, è possibile selezionare quali funzionalità della protezione permanente devono essere attivate:

- ***Chiedi prima di rimuovere le minacce*** (*attivata per impostazione predefinita*): selezionando questa opzione, Resident Shield non eseguirà alcuna azione automaticamente. Verrà invece visualizzata una finestra di dialogo che descrive la minaccia rilevata, consentendo di scegliere l'azione da eseguire. Se si mantiene deselezionata la casella, **AVG Internet Security 2013** tenterà automaticamente di correggere l'infezione e, nel caso sia impossibile, sposterà l'oggetto in Quarantena virus.

- ***Scansione dei cookie di rilevamento*** (*disattivata per impostazione predefinita*): questo parametro stabilisce che i cookie devono essere rilevati durante la scansione. (*I cookie HTTP sono utilizzati per autenticare, rilevare e mantenere informazioni specifiche sugli utenti, quali le preferenze dei siti e il contenuto dei carrelli elettronici.*)

- ***Segnala programmi potenzialmente indesiderati e minacce spyware***(*attivata per impostazione predefinita*): selezionare questa casella di controllo per attivare la scansione per ricercare spyware e virus. Gli spyware rappresentano una categoria di malware anomala: anche se solitamente costituiscono un rischio per la sicurezza, alcuni di questi programmi possono essere installati intenzionalmente. Si consiglia di mantenere questa funzionalità attivata in quanto consente di aumentare la protezione del computer.

- ***Segnala set potenziati di programmi potenzialmente indesiderati*** (*disattivata per impostazione predefinita*) : selezionare questa casella di controllo per rilevare pacchetti estesi di spyware, ovvero programmi perfettamente normali e innocui al momento dell'acquisto diretto presso il produttore, ma utilizzabili a scopi dannosi successivamente. Si tratta di una precauzione aggiuntiva che aumenta ulteriormente la protezione del

computer, ma che potrebbe bloccare programmi legittimi, pertanto l'opzione è disattivata per impostazione predefinita.

- ***Scansione alla chiusura*** (*disattivata per impostazione predefinita*): la scansione alla chiusura assicura che AVG esegua la scansione di oggetti attivi (ad esempio applicazioni, documenti e così via) quando vengono aperti e anche quando vengono chiusi. Questa funzionalità consente di proteggere il computer da alcuni tipi di virus sofisticati.

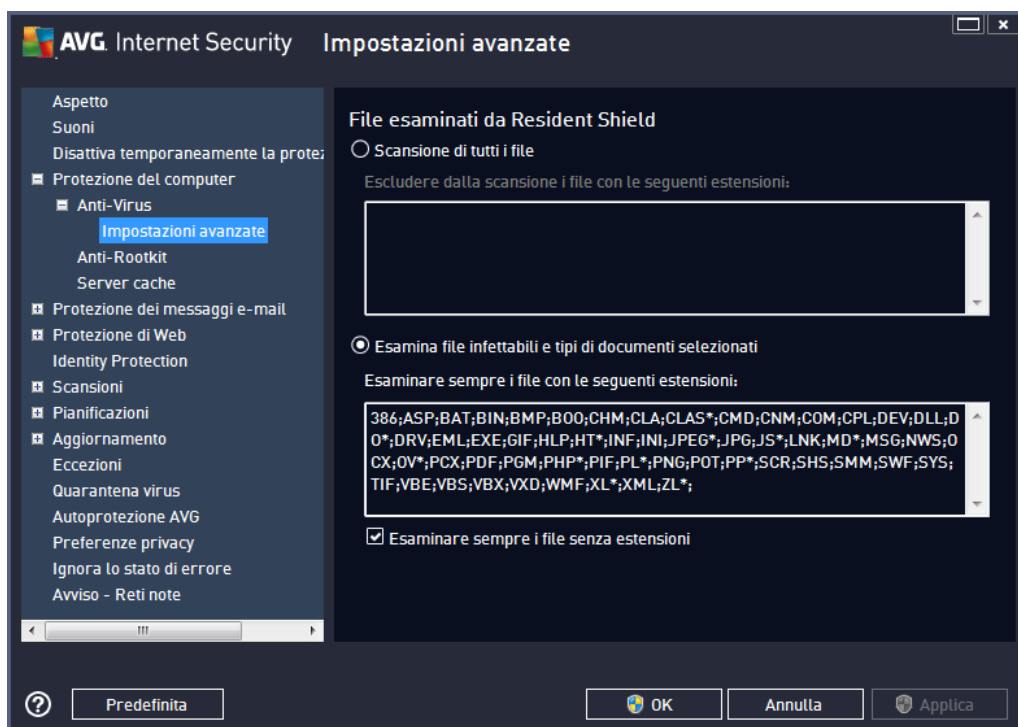
- ***Scansione settore di avvio di supporti rimovibili*** (*attivata per impostazione predefinita*)

- ***Usa analisi euristiche*** (*attivata per impostazione predefinita*): l'analisi euristica verrà utilizzata per il rilevamento (*emulazione dinamica delle istruzioni dell'oggetto sottoposto a scansione in un ambiente informatico virtuale*).

- ***Scansione file nominati nel registro*** (*attivata per impostazione predefinita*): questo parametro specifica che AVG sottoporrà a scansione tutti i file eseguibili aggiunti al registro di avvio per evitare che un'infezione nota venga eseguita al successivo avvio del computer.

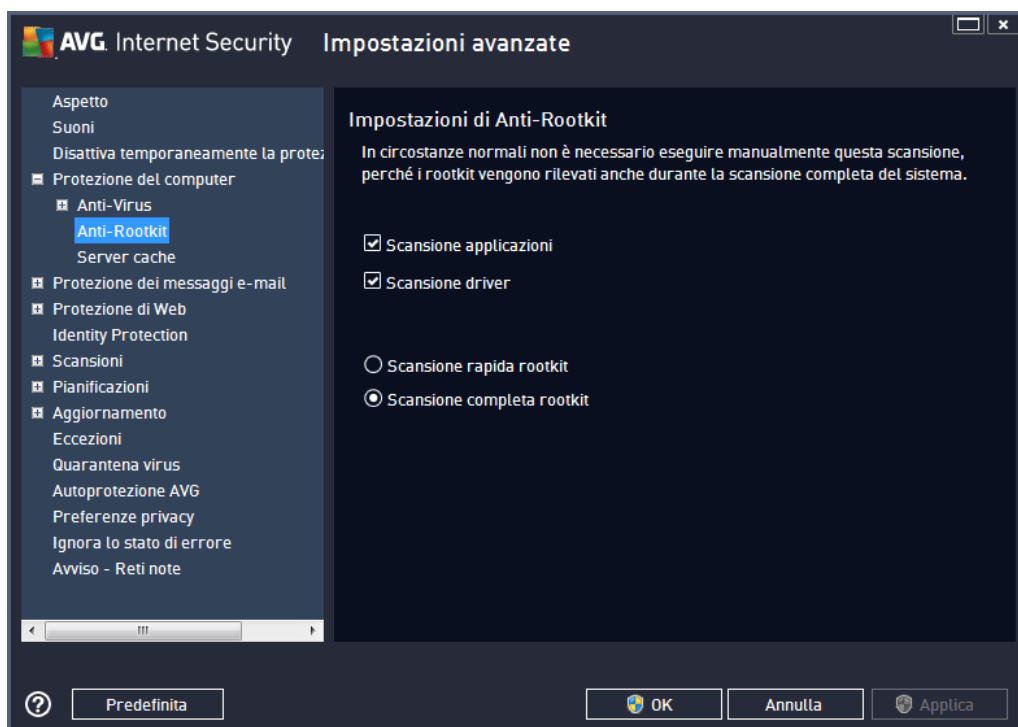
- ***Attiva scansione completa*** (*disattivata per impostazione predefinita*) : in situazioni specifiche (*stati di estrema emergenza*) è possibile selezionare questa opzione per attivare gli algoritmi di scansione più completi che esamineranno accuratamente tutti gli oggetti potenzialmente minacciosi. Tenere presente tuttavia che questo metodo è piuttosto dispendioso in termini di tempo.

- ***Attiva la protezione per la messaggistica immediata e i download P2P*** (*attivata per impostazione predefinita*) : selezionare questa voce se si desidera verificare che la comunicazione tramite messaggistica immediata (*ad esempio AIM, Yahoo!, ICQ, Skype, MSN Messenger e così via*) e i dati scaricati nelle reti peer-to-peer *(reti potenzialmente pericolose che consentono la connessione diretta tra client, senza un server, in genere sono utilizzate per condividere file musicali)* siano privi di virus.

Nella finestra di dialogo ***File esaminati da Resident Shield*** è possibile configurare i file che verranno sottoposti a scansione (*in base a estensioni specifiche*):

Selezionare la rispettiva casella di controllo per specificare se si desidera utilizzare l'opzione ***Scansione di tutti i file*** oppure solo ***Esamina file infettabili e tipi di documenti selezionati***. Per velocizzare la scansione e assicurare contemporaneamente il livello massimo di protezione, si consiglia di mantenere le impostazioni predefinite. In questo modo verranno sottoposti a scansione solo i file infettabili. Nella relativa sezione della finestra di dialogo è inoltre possibile trovare un elenco modificabile delle estensioni che definiscono i file inclusi nella scansione.

Selezionare l'opzione ***Esaminare sempre i file senza estensioni*** (*attivata per impostazione predefinita*) per assicurare che Resident Shield esegua anche la scansione dei file senza estensione e di formato sconosciuto. Si consiglia di mantenere questa funzionalità sempre attivata, in quanto i file senza estensione sono sospetti.

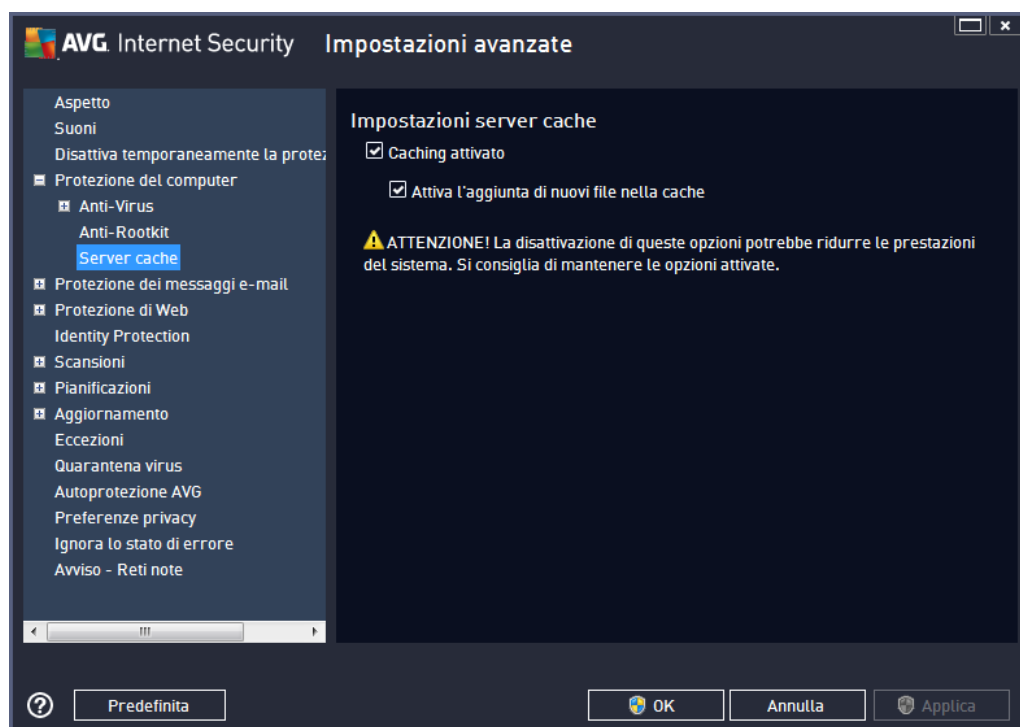
9.4.2. Anti-Rootkit

Nella finestra di dialogo ***Impostazioni di Anti-Rootkit*** è possibile modificare la configurazione del servizio ***Anti-Rootkit*** e i parametri specifici della scansione Anti-Rootkit. La scansione Anti-Rootkit è un processo predefinito incluso nella Scansione intero computer:

Scansione applicazioni e ***Scansione driver*** consentono di specificare in dettaglio gli elementi da includere nella scansione Anti-Rootkit. Queste impostazioni sono progettate per utenti esperti. Si consiglia di lasciare attivate tutte le opzioni. È inoltre possibile selezionare la modalità di scansione rootkit:

- ***Scansione rapida rootkit***: sottopone a scansione tutti i processi in esecuzione, i driver caricati e la cartella di sistema (*solitamente c:\Windows*)

- ***Scansione completa rootkit***: sottopone a scansione tutti i processi in esecuzione, i driver caricati e la cartella di sistema (*solitamente c:\Windows*), nonché tutte le unità locali (*inclusa l'unità di memoria flash, ma escluse le unità disco floppy/CD*)

9.4.3. Server cache

La finestra di dialogo ***Impostazioni del Server cache*** si riferisce al processo server cache destinato a velocizzare tutti i tipi di scansione di **AVG Internet Security 2013**:

Il server cache raccoglie e mantiene le informazioni relative ai file affidabili (*un file viene considerato affidabile se presenta la firma digitale di una fonte affidabile*). Questi file vengono quindi considerati sicuri e non necessitano di ulteriore scansione, pertanto vengono ignorati durante le scansioni.

La finestra di dialogo ***Impostazioni del Server cache*** offre le seguenti opzioni di configurazione:

- ***Caching attivato*** (*attivata per impostazione predefinita*) – deselezionare la casella per disattivare il ***Server cache*** e svuotare la memoria cache. Tenere presente che la scansione potrebbe subire un rallentamento e le prestazioni complessive del computer potrebbero ridursi, poiché per prima cosa ogni singolo file in uso verrà sottoposto alla scansione antivirus e antispyware.

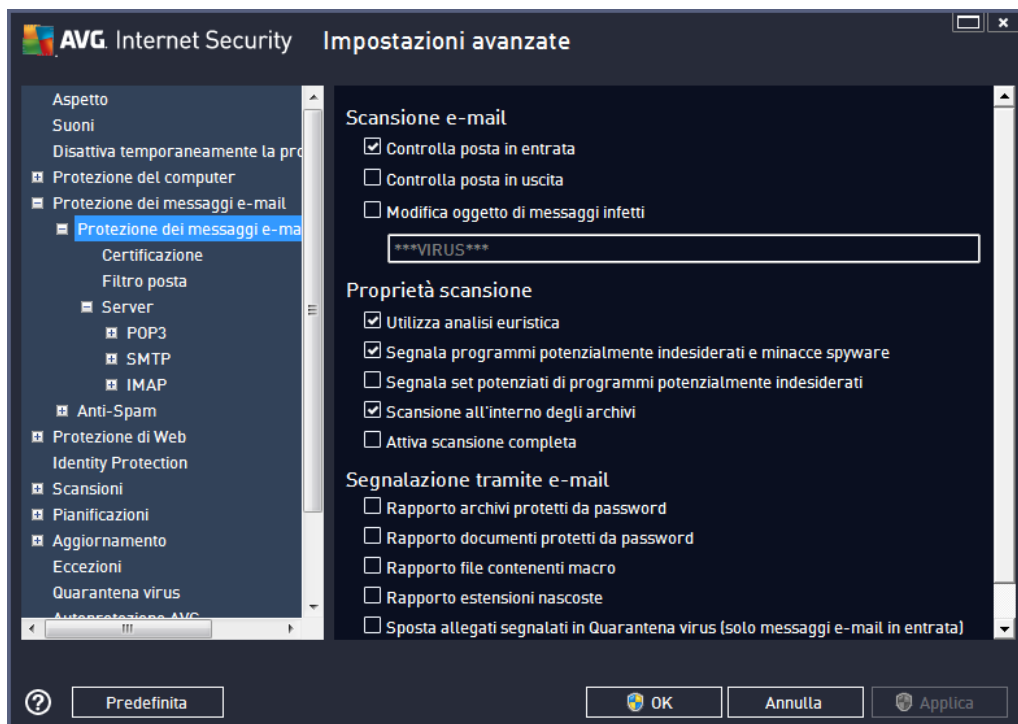
- ***Attiva l'aggiunta di nuovi file nella cache*** (*attivata per impostazione predefinita*) – deselezionare la casella per arrestare l'aggiunta di ulteriori file nella memoria cache. Tutti i file già presenti nella cache verranno mantenuti e utilizzati finché l'inserimento nella cache non verrà disattivato completamente o finché non verrà eseguito il successivo aggiornamento del database dei virus.

A meno che non sussista un motivo valido per disattivare il server cache, si consiglia di mantenere le impostazioni predefinite e lasciare attivate entrambe le opzioni. In caso contrario, la velocità e le prestazioni del sistema potrebbero ridursi notevolmente.

9.5. Scansione E-mail

In questa sezione è possibile modificare la configurazione dettagliata di Scansione E-mail e Anti-Spam:

9.5.1. Scansione E-mail

La finestra di dialogo ***Scansione E-mail*** è suddivisa in tre sezioni:

Scansione e-mail

In questa sezione è possibile configurare le seguenti impostazioni di base per i messaggi e-mail in arrivo e/o in uscita:

- ***Controlla posta in entrata*** (*attivata per impostazione predefinita*): selezionare per attivare/disattivare l'opzione di scansione di tutti i messaggi e-mail consegnati al client e-mail

- ***Controlla posta in uscita*** (*disattivata per impostazione predefinita*): selezionare per attivare/disattivare l'opzione di scansione di tutti i messaggi e-mail inviati dall'account e-mail

- ***Modifica oggetto di messaggi infetti*** (*disattivata per impostazione predefinita*): per essere informati del fatto che il messaggio e-mail sottoposto a scansione si è rivelato infetto, selezionare questa voce e immettere il testo desiderato nel campo di testo. Il testo verrà aggiunto al campo "Oggetto" di ogni messaggio rilevato come infetto per facilitarne l'identificazione e il filtro. Il valore predefinito è ***VIRUS***. Si consiglia di mantenere questo valore.

Proprietà scansione

In questa sezione è possibile specificare la modalità di scansione dei messaggi e-mail:

- ***Usa analisi euristiche*** (*attivata per impostazione predefinita*): selezionare questa opzione per utilizzare il metodo di rilevamento tramite analisi euristica durante la scansione dei messaggi e-mail. Se questa opzione è attivata, è possibile filtrare gli allegati dei messaggi e-mail non solo per estensione ma anche in base al contenuto effettivo dell'allegato. Il filtro può essere impostato nella finestra di dialogo Filtro posta.

- ***Segnala programmi potenzialmente indesiderati e minacce spyware*** (*attivata per impostazione predefinita*): selezionare questa casella di controllo per attivare la scansione per ricercare spyware e virus. Gli spyware rappresentano una categoria di malware anomala: anche se solitamente costituiscono un rischio per la sicurezza, alcuni di questi programmi possono essere installati intenzionalmente. Si consiglia di mantenere questa funzionalità attivata in quanto consente di aumentare la protezione del computer.

- ***Segnala set potenziati di programmi potenzialmente indesiderati*** (*disattivata per impostazione predefinita*): selezionare questa casella di controllo per rilevare pacchetti estesi di spyware, ovvero programmi perfettamente normali e innocui al momento dell'acquisto diretto presso il produttore, ma utilizzabili a scopi dannosi successivamente. Si tratta di una precauzione aggiuntiva che aumenta ulteriormente la protezione del computer, ma che potrebbe bloccare programmi legittimi, pertanto l'opzione è disattivata per impostazione predefinita.

- ***Scansione all'interno degli archivi*** (*attivata per impostazione predefinita*): selezionare questa casella di controllo per eseguire la scansione del contenuto degli archivi allegati ai messaggi e-mail.

- ***Attiva scansione completa*** (*disattivata per impostazione predefinita*): in situazioni specifiche (*ad esempio se si sospetta che il computer sia stato infettato da un virus o un attacco*) per maggiore sicurezza è possibile selezionare questa opzione per attivare gli algoritmi di scansione più completi che esamineranno anche le aree del computer che difficilmente vengono infettate. Tenere presente tuttavia che questo metodo è piuttosto dispendioso in termini di tempo.

Segnalazione allegati e-mail

In questa sezione, è possibile impostare rapporti aggiuntivi sui file potenzialmente pericolosi o sospetti. Tenere presente che non verrà visualizzato alcun messaggio di avviso, verrà aggiunto soltanto un testo di certificazione alla fine del messaggio e-mail e tutti i rapporti verranno elencati nella finestra di dialogo Rilevamento Scansione E-mail:

- ***Segnala archivi protetti da password***: gli archivi (*ZIP, RAR e così via*) protetti da password non possono essere sottoposti alla scansione antivirus. Selezionare la casella di controllo se si desidera che questi file vengano segnalati come potenzialmente pericolosi.

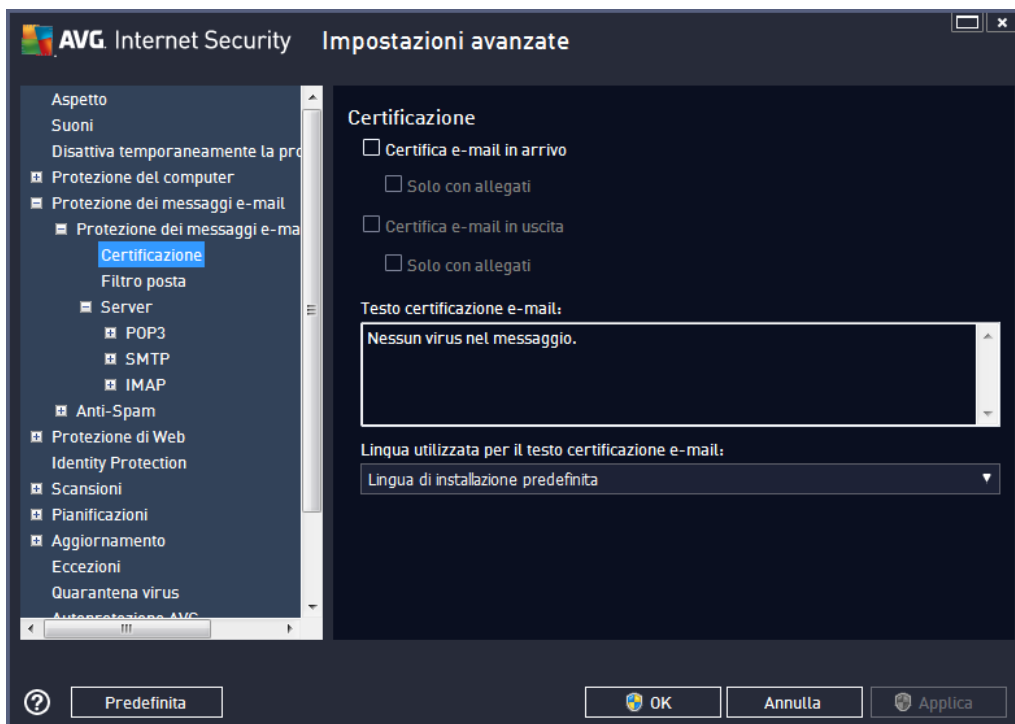
- ***Segnala documenti protetti da password*** : i documenti protetti da password non possono essere sottoposti alla scansione antivirus. Selezionare la casella di controllo se si desidera che questi file vengano segnalati come potenzialmente pericolosi.

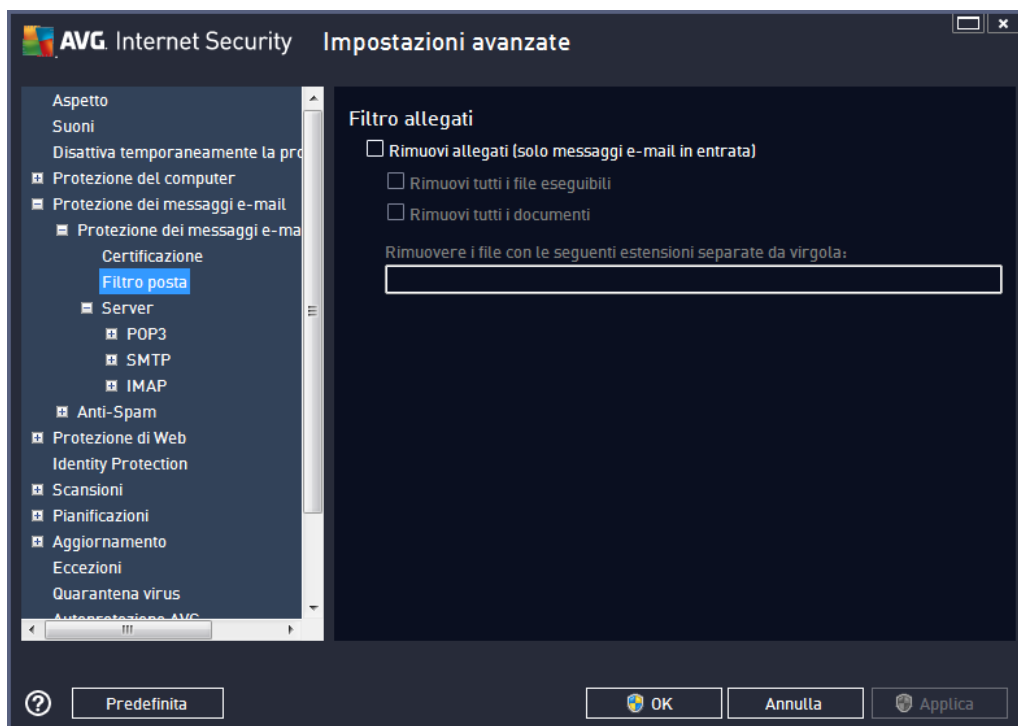
- ***Segnala file contenenti macro***: una macro è una sequenza di passaggi predefinita che consente di semplificare determinate attività (*le macro di MS Word, ad esempio, sono ampiamente conosciute*). Le macro possono contenere istruzioni potenzialmente

pericolose. Selezionare la casella di controllo per assicurare che i file contenenti macro vengano segnalati come potenzialmente pericolosi.

- ***Segnala estensioni nascoste***: le estensioni nascoste possono far sembrare un file sospetto, ovvero un file eseguibile del tipo "nomefile.txt.exe", come un innocuo file di testo del tipo "nomefile.txt". Selezionare la casella di controllo se si desidera che questi file vengano segnalati come potenzialmente pericolosi.

- ***Sposta allegati segnalati in Quarantena virus***: consente di specificare se si desidera ricevere una notifica via e-mail per gli archivi protetti da password, i documenti protetti da password, i file contenenti macro e/o i file con estensione nascosta rilevati come allegato del messaggio e-mail sottoposto a scansione. Se viene identificato un messaggio simile durante la scansione, è possibile stabilire se l'oggetto infetto rilevato deve essere spostato in Quarantena virus.

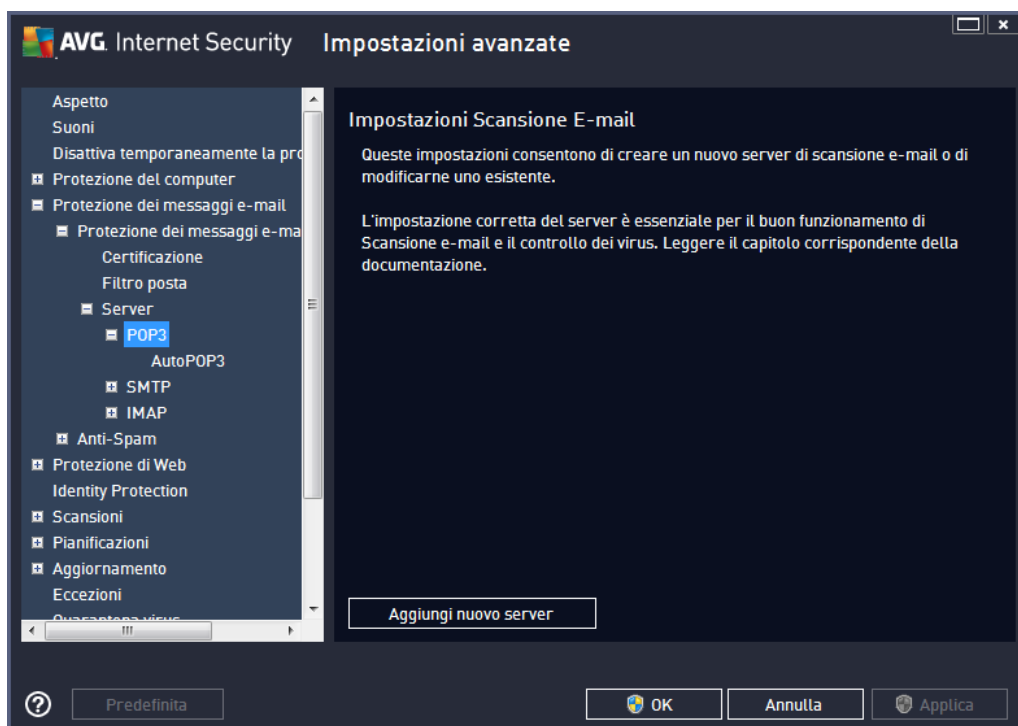
Nella finestra di dialogo ***Certificazione*** è possibile selezionare le caselle di controllo specifiche per specificare se si desidera certificare la posta in arrivo (***Certifica e-mail in arrivo***) e/o la posta in uscita (***Certifica e-mail in uscita***). Per ciascuna di queste opzioni è inoltre possibile specificare il parametro ***Solo con allegati*** per far sì che la certificazione venga aggiunta solo ai messaggi e-mail con allegati:

Per impostazione predefinita, il testo di certificazione è composto da informazioni di base simili a *Nessun virus in questo messaggio.* Tuttavia, è possibile estendere o modificare queste informazioni in base alle esigenze, scrivendo il testo di certificazione desiderato nel campo ***Testo certificazione e-mail***. Nella sezione ***Lingua utilizzata per il testo certificazione e-mail*** è possibile inoltre definire in quale lingua verrà visualizzata la parte di certificazione generata automaticamente (*Nessun virus in questo messaggio*).

Nota: *tenere presente che solo il testo predefinito verrà visualizzato nella lingua richiesta e il testo personalizzato non verrà tradotto automaticamente.*

La finestra di dialogo ***Filtro allegati*** consente di impostare i parametri per la scansione degli allegati ai messaggi e-mail**.** Per impostazione predefinita, l'opzione ***Rimuovi allegati*** è disattivata. Se si decide di attivarla, tutti gli allegati ai messaggi e-mail rilevati come infetti o potenzialmente pericolosi verranno rimossi automaticamente. Se si desidera definire tipi specifici di allegati che devono essere rimossi, selezionare l'opzione corrispondente:

- ***Rimuovi tutti i file eseguibili***: tutti i file *.exe verranno eliminati
- ***Rimuovi tutti i documenti***: tutti i file *.doc, *.docx, *.xls e *.xlsx verranno eliminati
- ***Rimuovere i file con le seguenti estensioni separate da virgola***: verranno rimossi tutti i file con le estensioni specificate

Nella sezione ***Server*** è possibile modificare i parametri dei server di Scansione E-mail:

- Server POP3
- Server SMTP
- Server IMAP

Inoltre, è possibile definire nuovi server per la posta in arrivo o in uscita, utilizzando il pulsante ***Aggiungi nuovo server***.

Questa finestra di dialogo (*che si apre da **Server / POP3***) consente di impostare un nuovo server di Scansione E-mail utilizzando il protocollo POP3 per la posta in entrata:

- ***Nome server POP3***: in questo campo è possibile specificare il nome dei nuovi server aggiunti (*per aggiungere un server POP3, fare clic con il pulsante destro del mouse sulla voce POP3 nel menu di esplorazione a sinistra*). Per i server "AutoPOP3" creati automaticamente questo campo è disattivato.

- ***Tipo di accesso***: definisce il metodo per determinare il server e-mail utilizzato per la posta in arrivo:

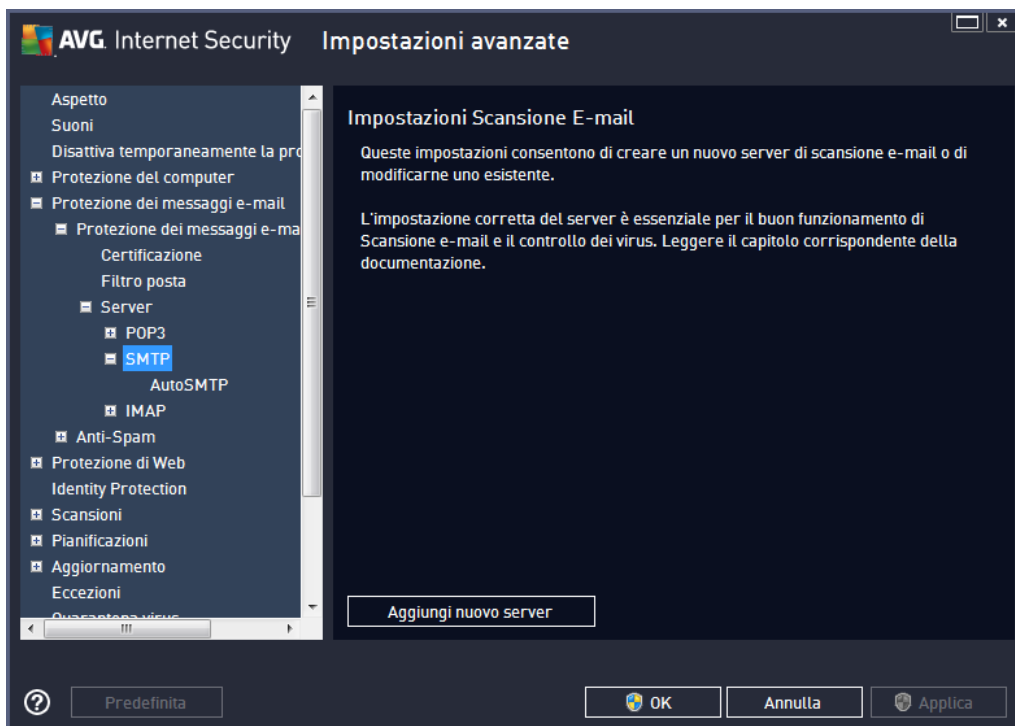
  - ***Automatico***: l'accesso verrà effettuato automaticamente, in base alle impostazioni del client e-mail.

  - ***Host fisso***: in questo caso verrà sempre utilizzato il server specificato in questo campo. Specificare l'indirizzo o il nome del server e-mail. Il nome di accesso non verrà modificato. Per il nome, è possibile utilizzare un nome di dominio (*ad esempio pop.acme.com*) o un indirizzo IP (*ad esempio 123.45.67.89*). Se il server e-mail utilizza una porta non standard, è possibile specificare il nome della porta dopo quello del server utilizzando come separatore il segno di due punti, (*ad esempio pop.acme.com:8200*). La porta standard per la comunicazione POP3 è la numero 110.

- ***Altre impostazioni***: specifica parametri più dettagliati:

  - ***Porta locale***: specifica la porta su cui è prevista la comunicazione dall'applicazione e-mail. Nell'applicazione e-mail sarà quindi necessario specificare tale porta come porta per la comunicazione POP3.

- o ***Connessione***: nel menu a discesa è possibile specificare il tipo di connessione da utilizzare (*regolare/SSL/SSL predefinito*). Se si sceglie la connessione SSL, i dati inviati verranno crittografati senza il rischio di essere rilevati o monitorati da terzi. Questa funzionalità inoltre è disponibile solo se supportata dal server e-mail di destinazione.

- ***Attivazione server POP3 client e-mail***: selezionare/deselezionare questa voce per attivare o disattivare il server POP3 specificato

Questa finestra di dialogo (*che si apre tramite **Server / SMTP***) consente di impostare un nuovo server di Scansione E-mail che utilizza il protocollo SMTP per la posta in uscita:

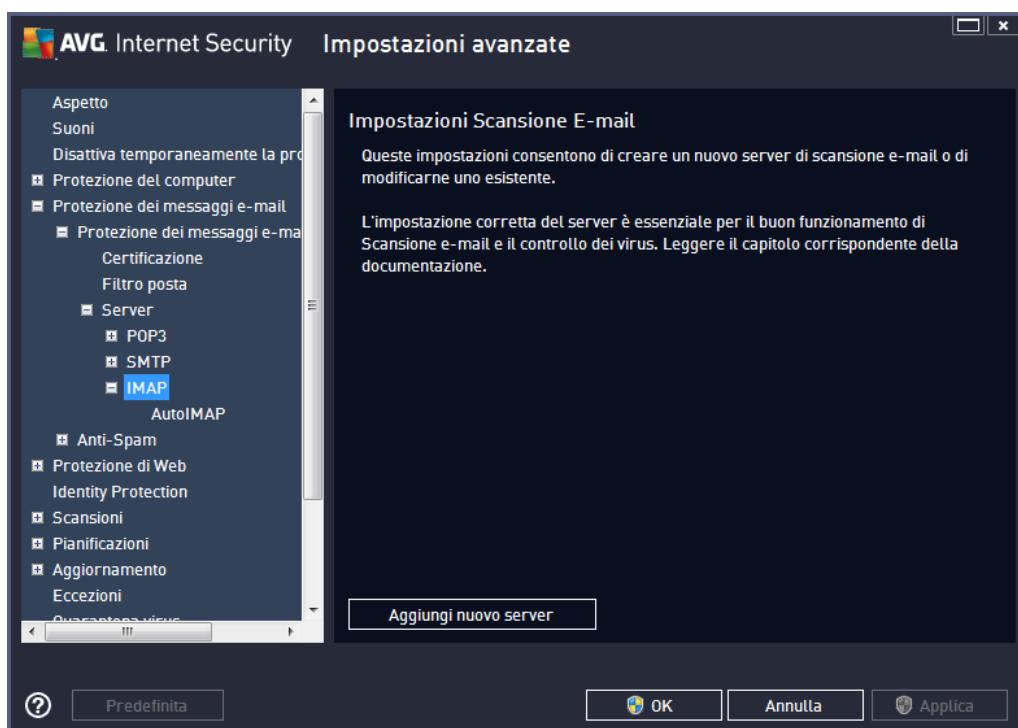
- ***Nome server SMTP***: in questo campo è possibile specificare il nome dei nuovi server aggiunti (*per aggiungere un server SMTP, fare clic con il pulsante destro del mouse sulla voce SMTP nel menu di esplorazione a sinistra*). Per i server "AutoSMTP" creati automaticamente questo campo è disattivato.

- ***Tipo di accesso***: definisce il metodo per determinare il server e-mail utilizzato per la posta in uscita:

  - o ***Automatico***: l'accesso verrà effettuato automaticamente, in base alle impostazioni del client e-mail

  - o ***Host fisso***: in questo caso verrà sempre utilizzato il server specificato in questo campo. Specificare l'indirizzo o il nome del server e-mail. Per il nome, è possibile utilizzare un nome di dominio (*ad esempio imap.acme.com*) o un indirizzo IP (*ad esempio 123.45.67.89*). Se il server e-mail utilizza una porta non standard, è possibile digitare il nome della porta dopo quello del server utilizzando come

separatore il segno di due punti, *ad esempio smtp.acme.com:8200*. La porta standard per la comunicazione SMTP è la numero 25.

- ***Altre impostazioni***: specifica parametri più dettagliati:
  - o ***Porta locale***: specifica la porta su cui è prevista la comunicazione dall'applicazione e-mail. Nell'applicazione e-mail sarà quindi necessario specificare tale porta come porta per la comunicazione SMTP.
  - o ***Connessione***: questo menu a discesa consente di specificare il tipo di connessione da utilizzare (*normale/SSL/SSL predefinito*). Se si sceglie la connessione SSL, i dati inviati verranno crittografati senza il rischio di essere rilevati o monitorati da terzi. Questa funzionalità è disponibile solo se supportata dal server e-mail di destinazione.
- ***Attivazione server SMTP per client e-mail***: selezionare/deselezionare questa casella per attivare/disattivare il server SMTP specificato sopra

Questa finestra di dialogo (accessibile tramite ***Server / IMAP***) consente di impostare un nuovo server Scansione E-mail che utilizza il protocollo IMAP per la posta in uscita:

- ***Nome server IMAP***: in questo campo è possibile specificare il nome dei nuovi server aggiunti (*per aggiungere un server IMAP, fare clic con il pulsante destro del mouse sulla voce IMAP nel menu di esplorazione a sinistra*). Per i server "AutoIMAP" creati automaticamente questo campo è disattivato.
- ***Tipo di accesso***: definisce il metodo per determinare il server e-mail utilizzato per la posta in uscita:
  - o ***Automatico***: l'accesso verrà effettuato automaticamente, in base alle impostazioni

del client e-mail

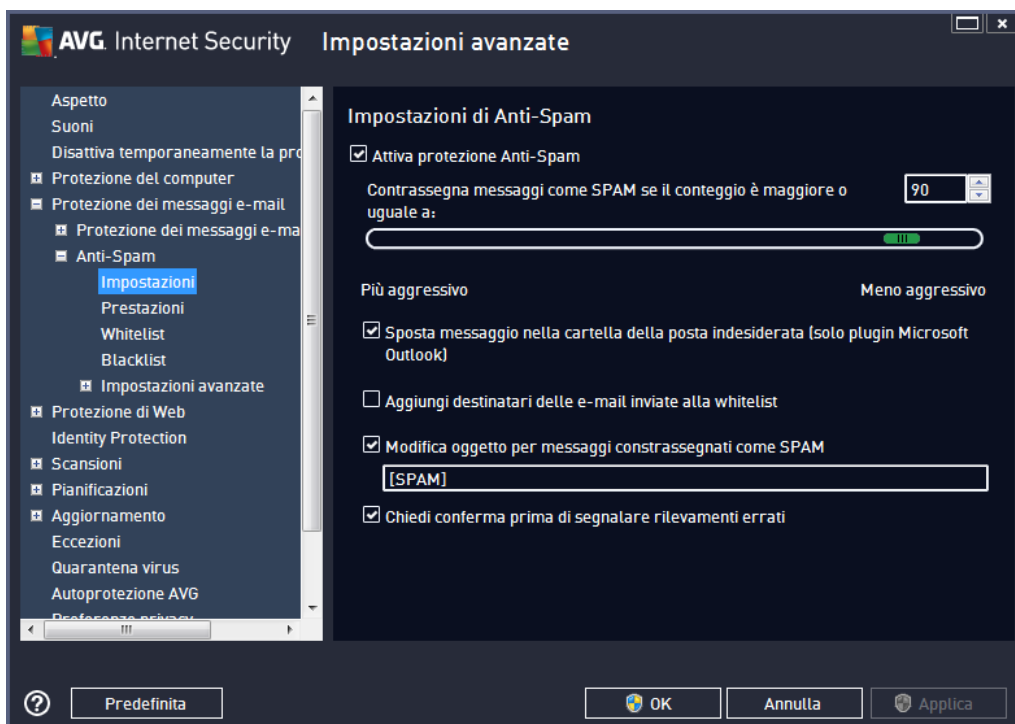
- o ***Host fisso***: in questo caso verrà sempre utilizzato il server specificato in questo campo. Specificare l'indirizzo o il nome del server e-mail. Per il nome, è possibile utilizzare un nome di dominio (*ad esempio imap.acme.com*) o un indirizzo IP (*ad esempio 123.45.67.89*). Se il server e-mail utilizza una porta non standard, è possibile digitare il nome della porta dopo quello del server utilizzando come separatore il segno di due punti, *ad esempio imap.acme.com:8200.* La porta standard per la comunicazione IMAP è la numero 143.

- ***Altre impostazioni***: specifica parametri più dettagliati:

  - o ***Porta locale***: specifica la porta su cui è prevista la comunicazione dall'applicazione e-mail. Nell'applicazione e-mail sarà quindi necessario specificare tale porta come porta per la comunicazione IMAP.

  - o ***Connessione***: questo menu a discesa consente di specificare il tipo di connessione da utilizzare (*normale/SSL/SSL predefinito*). Se si sceglie la connessione SSL, i dati inviati verranno crittografati senza il rischio di essere rilevati o monitorati da terze parti. Questa funzionalità è disponibile solo se supportata dal server e-mail di destinazione.

- ***Attivazione server IMAP per client e-mail***: selezionare/deselezionare questa casella per attivare/disattivare il server IMAP specificato sopra

9.5.2. Anti-Spam

Nella finestra di dialogo delle ***impostazioni Anti-Spam*** è possibile selezionare/deselezionare la casella di controllo ***Attiva protezione Anti-Spam*** per consentire/impedire la scansione anti-spam delle comunicazioni e-mail. Questa opzione è attivata per impostazione predefinita e si consiglia di non modificare questa impostazione a meno che non siano presenti motivi validi per farlo.

Quindi, è anche possibile selezionare il grado di "aggressività" della configurazione del conteggio. Il filtro ***Anti-Spam*** assegna a ciascun messaggio un conteggio (*ad esempio, il grado di somiglianza del contenuto del messaggio a SPAM*) in base a diverse tecniche di scansione dinamica. È possibile regolare l'impostazione ***Contrassegna messaggio come spam se il conteggio è maggiore di*** digitando il valore oppure spostando il dispositivo di scorrimento verso sinistra o verso destra (*l'intervallo di valori è compreso tra 50 e 90*).

Si consiglia in genere di impostare la soglia tra 50 e 90 oppure, se non si è sicuri, su 90. Di seguito viene fornita una panoramica generale della soglia di conteggio:

- ***Valore compreso tra 80 e 90***: verranno filtrati i messaggi e-mail il cui contenuto è probabilmente spam, ma potrebbero essere filtrati anche alcuni messaggi che non ne contengono.

- ***Valore tra 60 e 79***: è considerata una configurazione abbastanza "aggressiva". Verranno filtrati i messaggi e-mail il cui contenuto potrebbe essere spam, ma potrebbero essere filtrati anche messaggi che non ne contengono.

- ***Valore tra 50 e 59***: configurazione particolarmente aggressiva. È probabile che insieme ai messaggi e-mail contenenti spam vengano filtrati anche i messaggi normali. Questo intervallo di valori non è consigliato per l'uso normale.

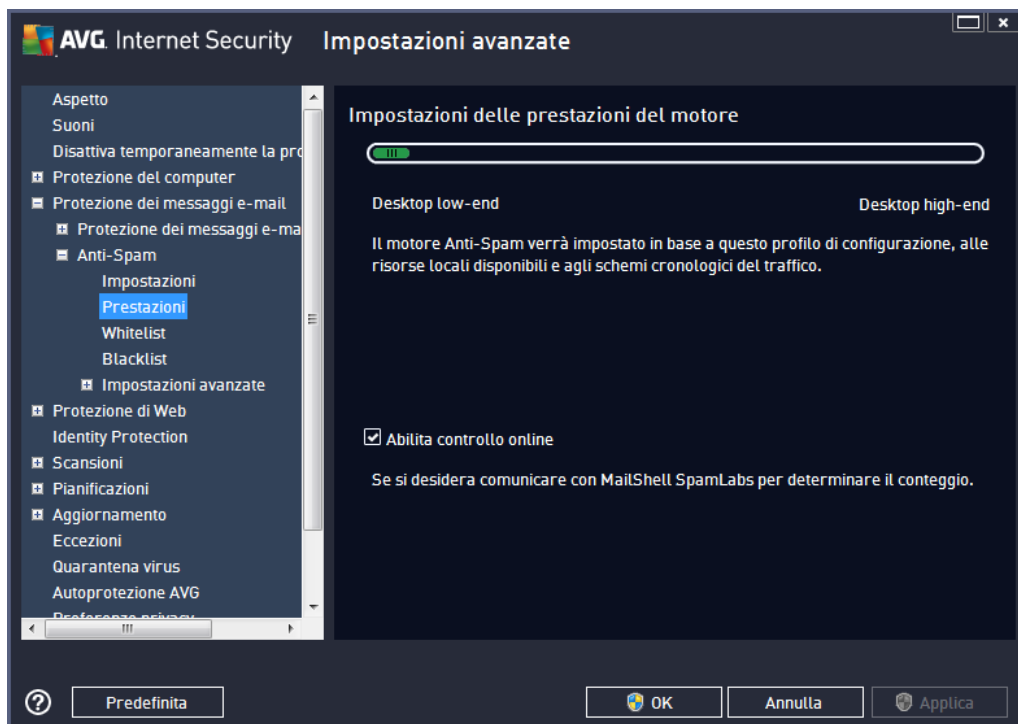
Nella finestra di dialogo delle ***impostazioni Anti-Spam*** è possibile definire ulteriormente la modalità di gestione dei messaggi e-mail di spam:

- ***Sposta messaggio nella cartella della posta indesiderata*** *(solo plugin Microsoft Outlook)*: selezionare questa casella di controllo per specificare che ciascun messaggio di spam rilevato deve essere automaticamente spostato nella cartella specifica della posta indesiderata all'interno del client e-mail Microsoft Outlook. Al momento, questa funzione non è supportata in altri client e-mail.

- ***Aggiungi destinatari delle e-mail inviate alla whitelist***: selezionare questa casella di controllo per confermare che tutti i destinatari delle e-mail inviate sono affidabili e tutte le e-mail provenienti dai relativi account e-mail possono essere recapitate.

- ***Modifica oggetto per messaggi contrassegnati come SPAM***: selezionare questa casella di controllo se si desidera che tutti i messaggi rilevati come spam vengano contrassegnati con una parola o un carattere specifico nel campo dell'oggetto del messaggio e-mail. Il testo desiderato può essere digitato nel campo di testo attivato.

- ***Chiedi conferma prima di segnalare rilevamenti errati***: se durante il processo di installazione si è scelto di partecipare al progetto Preferenze privacy, si è acconsentito a segnalare le minacce rilevate a AVG. Il rilevamento viene eseguito automaticamente. È tuttavia possibile selezionare questa casella di controllo per specificare se si desidera che venga richiesta una conferma prima della segnalazione ad AVG dell'eventuale spam rilevato, in modo da assicurarsi che il messaggio debba effettivamente essere classificato come spam.

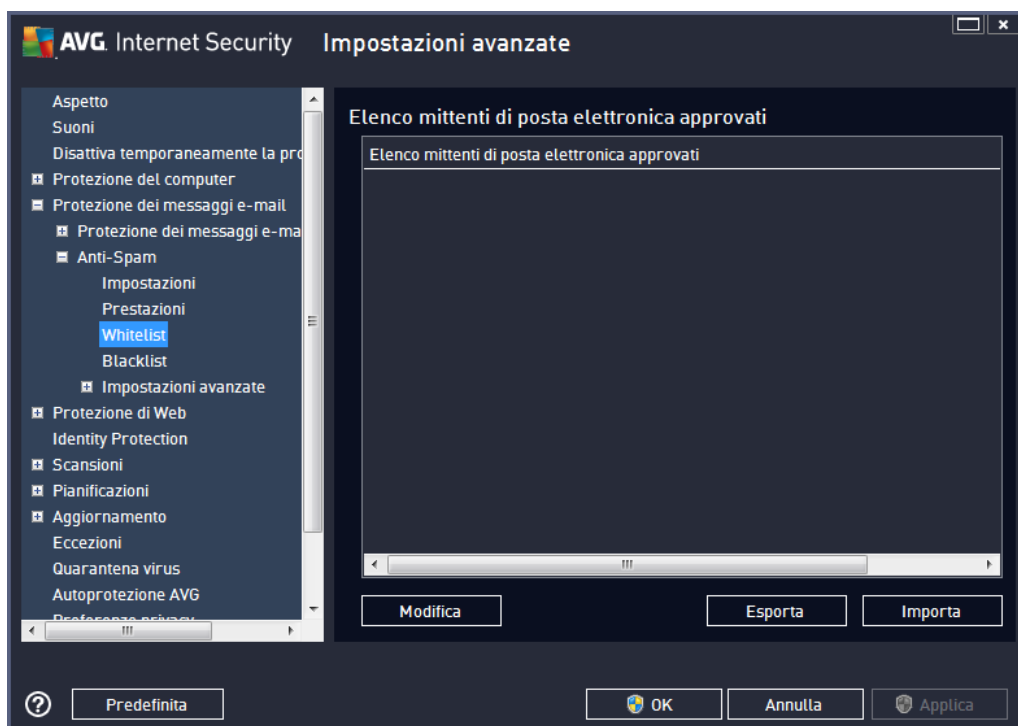
La finestra di dialogo ***Impostazioni delle prestazioni del motore*** (*accessibile dalla voce **Prestazioni** della struttura di esplorazione visualizzata a sinistra*) include le impostazioni delle prestazioni del componente ***Anti-Spam:***

Spostare il dispositivo di scorrimento a sinistra o a destra per modificare il livello dell'intervallo delle prestazioni di scansione tra le modalità ***Desktop low-end*** / ***Desktop high-end***.

- ***Desktop low-end***: durante il processo di scansione per l'identificazione dello spam, non viene utilizzata alcuna regola. Per l'identificazione dello spam verranno utilizzati solo i dati di formazione. Questa modalità non è consigliata, a meno che l'hardware del computer non sia estremamente limitato.

- ***Desktop high-end***: questa modalità richiederà una notevole quantità di memoria. Durante il processo di scansione per l'identificazione dello spam verranno utilizzate le seguenti funzionalità: regole e cache del database di spam, regole di base e avanzate, indirizzi IP e database di spammer.

La voce ***Abilita controllo on-line*** è attiva per impostazione predefinita. Ne risulta un rilevamento dello spam più preciso tramite la comunicazione con i server Mailshell, ovvero i dati sottoposti a scansione verranno confrontati con i database Mailshell in linea.

In genere si consiglia di mantenere le impostazioni predefinite e di modificarle solo se esiste un reale motivo per farlo. Le eventuali modifiche alla configurazione devono essere eseguite solo da utenti esperti.

La voce ***Whitelist*** consente di aprire la finestra di dialogo ***Elenco mittenti di posta elettronica approvati*** con un elenco globale di nomi di dominio e indirizzi e-mail approvati i cui messaggi non verranno mai contrassegnati come spam.

Nell'interfaccia di modifica è possibile compilare un elenco di mittenti da cui si ha la certezza che non verranno mai inviati messaggi indesiderati (spam). È inoltre possibile compilare un elenco di nomi di dominio completi (*ad esempio avg.com*) che non generano mai messaggi spam. Dopo che è stato preparato un simile elenco di mittenti e/o nomi di dominio, è possibile inserirli in due modi diversi: inserendo direttamente ciascun indirizzo e-mail o importando tutto l'elenco di indirizzi.

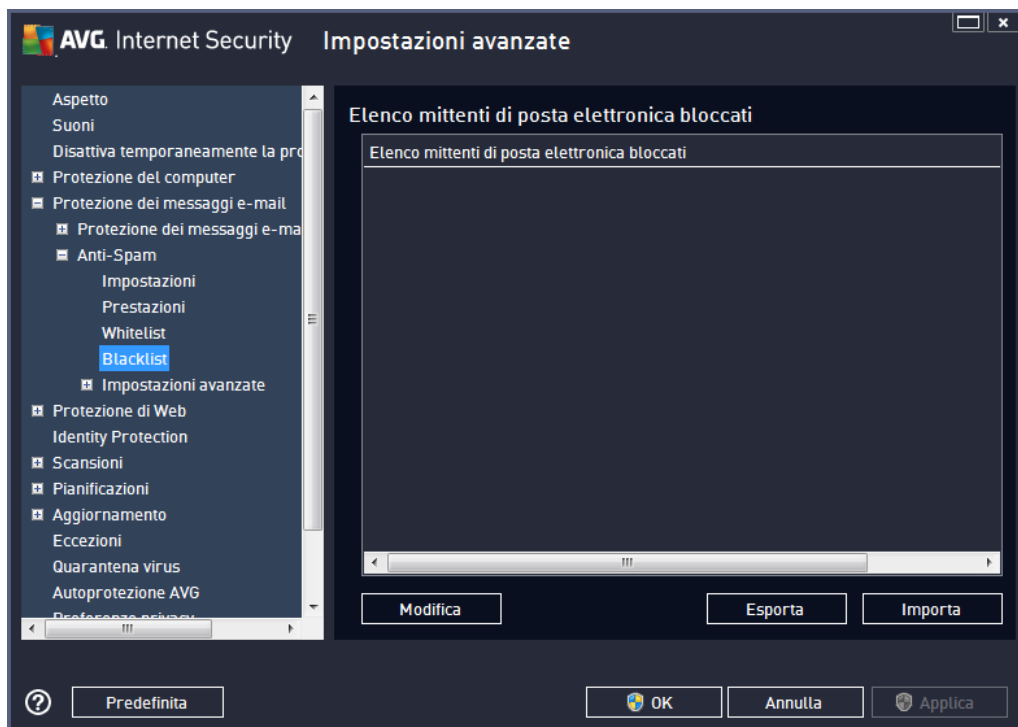
Pulsanti di controllo

Sono disponibili i seguenti pulsanti di controllo:

- ***Modifica***: selezionare questo pulsante per aprire una finestra di dialogo in cui è possibile immettere manualmente un elenco di indirizzi (*è inoltre possibile utilizzare il metodo copia e incolla*). Immettere una voce (*mittente o nome di dominio*) per riga.

- ***Esporta***: se per qualsiasi motivo si decide di esportare i record, è possibile fare clic su questo pulsante per eseguire l'operazione. Tutti i record verranno salvati in un file di testo normale.

- ***Importa***: se si possiede già un file di testo di indirizzi di posta elettronica o nomi di dominio, è possibile importare tale file selezionando questo pulsante. Il file deve includere una sola voce (*indirizzo, nome di dominio*) per riga.

La voce ***Blacklist*** consente di aprire una finestra di dialogo contenente un elenco globale di nomi di dominio e indirizzi e-mail di mittenti bloccati i cui messaggi saranno sempre contrassegnati come spam.

Nell'interfaccia di modifica è possibile compilare un elenco di mittenti da cui si ha la certezza di ricevere messaggi indesiderati *(spam)*. È inoltre possibile compilare un elenco di nomi di dominio completi (*ad esempio aziendaspam.com*) da cui si prevede di ricevere o si ricevono messaggi di spam. Tutti i messaggi e-mail ricevuti da tali indirizzi o domini specifici verranno contrassegnati come spam. Dopo che è stato preparato un simile elenco di mittenti e/o nomi di dominio, è possibile inserirli in due modi diversi: inserendo direttamente ciascun indirizzo e-mail o importando tutto l'elenco di indirizzi.

Pulsanti di controllo

Sono disponibili i seguenti pulsanti di controllo:

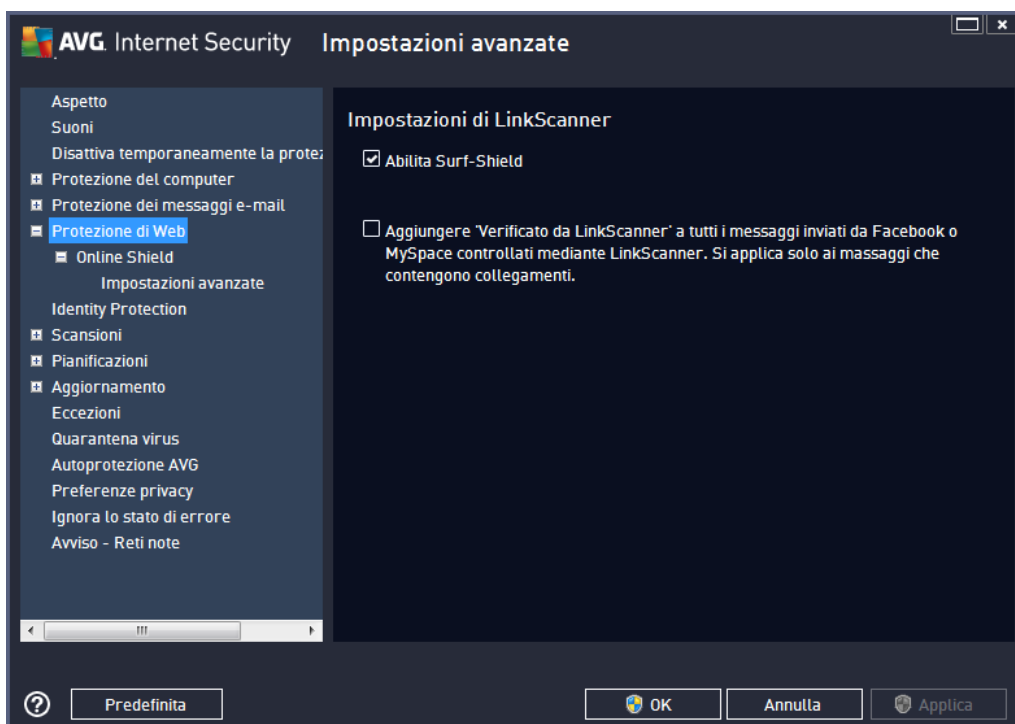
- ***Modifica***: selezionare questo pulsante per aprire una finestra di dialogo in cui è possibile immettere manualmente un elenco di indirizzi (è *inoltre possibile utilizzare il metodo copia e incolla*). Immettere una voce (*mittente o nome di dominio*) per riga.
- ***Esporta***: se per qualsiasi motivo si decide di esportare i record, è possibile fare clic su questo pulsante per eseguire l'operazione. Tutti i record verranno salvati in un file di testo normale.
- ***Importa***: se si possiede già un file di testo di indirizzi di posta elettronica o nomi di dominio, è possibile importare tale file selezionando questo pulsante.

Il ramo Impostazioni avanzate contiene opzioni di impostazione complete per la funzione Anti-Spam. Queste impostazioni sono destinate esclusivamente agli utenti esperti, in particolare agli amministratori di rete che devono eseguire una configurazione dettagliata della protezione anti-spam per garantire la massima protezione dei server e-mail. Per questo motivo non è disponibile una guida aggiuntiva nelle singole finestre di dialogo. Tuttavia, è disponibile direttamente nell'interfaccia utente una breve descrizione di ciascuna opzione. Si consiglia di non modificare alcuna impostazione a meno che non si abbiano familiarità con tutte le impostazioni avanzate di Spamcatcher (MailShell Inc.). Eventuali modifiche inappropriate possono dare luogo a una riduzione delle prestazioni o a un funzionamento errato del componente.

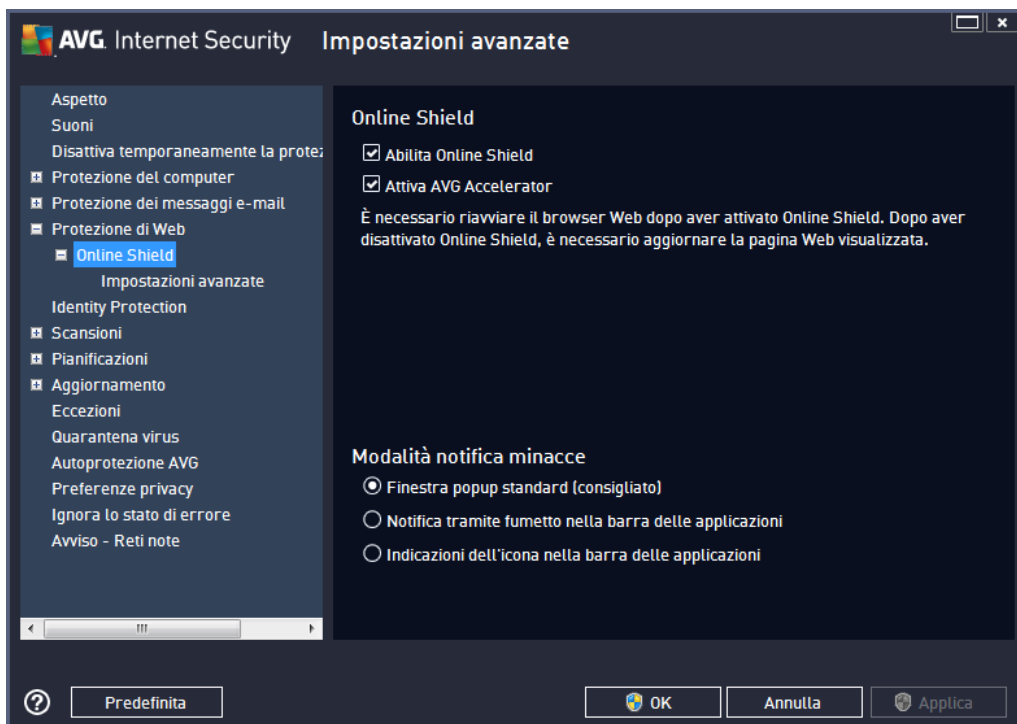
Se si ritiene di dover modificare comunque la configurazione Anti-Spam a un livello molto avanzato, seguire le istruzioni fornite direttamente nell'interfaccia utente. In genere, in ciascuna finestra di dialogo è contenuta una sola funzionalità specifica che può essere modificata. La relativa descrizione è sempre inclusa nella finestra di dialogo. È possibile modificare i seguenti parametri:

- ***Filtraggio***: elenco lingue, elenco paesi, IP approvati, IP bloccati, paesi bloccati, set di caratteri bloccati, mittenti contraffatti
- ***RBL***: server RBL, multihit, soglia, timeout, IP massimi
- ***Connessione Internet***: timeout, server proxy, autenticazione proxy

9.6. Protezione della navigazione sul Web

La finestra di dialogo ***Impostazioni LinkScanner*** consente di attivare/disattivare le seguenti funzioni:

- ***Abilita Surf-Shield***: (*attivata per impostazione predefinita*): protezione attiva, *in tempo reale,* da siti dannosi al momento dell'accesso. Le connessioni a siti dannosi noti e il relativo contenuto vengono bloccati non appena l'utente esegue l'accesso mediante un browser Web (*o qualsiasi altra applicazione che utilizza HTTP*).

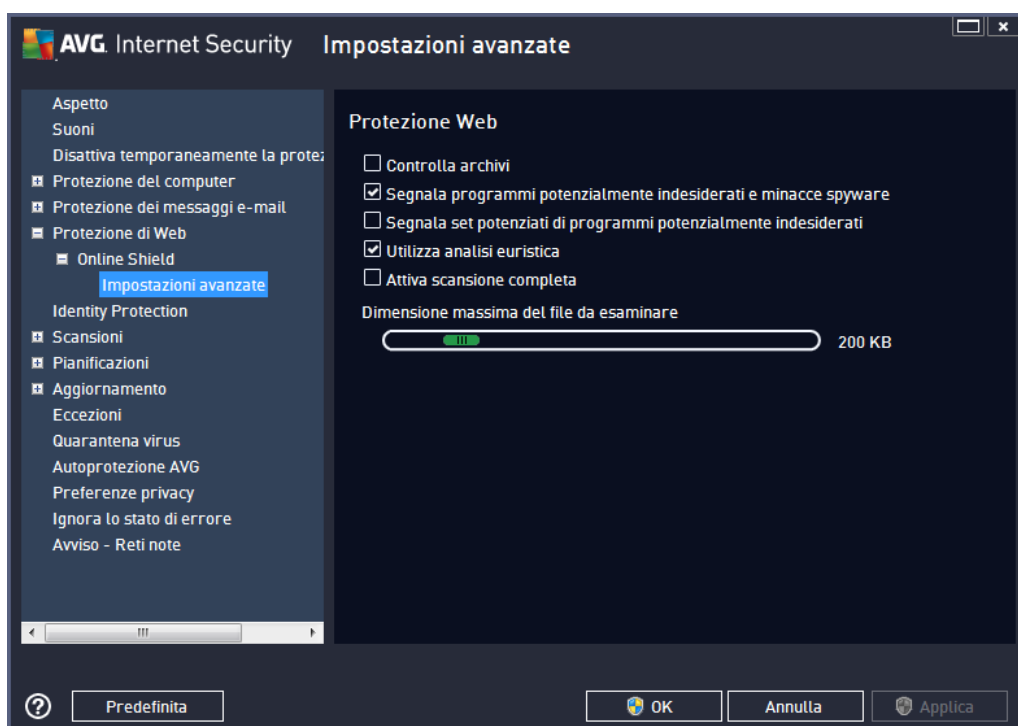
- ***Aggiungi "Verificato da LinkScanner"...***: (*disattivata per impostazione predefinita*): selezionare questa opzione per confermare che si desidera inserire un avviso di certificazione relativo al controllo LinkScanner in tutti i messaggi contenenti collegamenti ipertestuali attivi inviati dai social network Facebook e MySpace.

9.6.1. Online Shield

La finestra di dialogo ***Online Shield*** presenta le seguenti opzioni:

- ***Abilita Online Shield*** *(attivata per impostazione predefinita)*: attiva/disattiva l'intero servizio ***Online Shield***. Per ulteriori impostazioni avanzate di ***Online Shield***, passare alla successiva finestra di dialogo denominata Protezione Web.

- ***Attiva AVG Accelerator*** *(attivata per impostazione predefinita):* consente di attivare/disattivare il servizio AVG Accelerator. AVG Accelerator ottimizza la riproduzione dei video in linea e semplifica il download. Quando il processo di accelerazione video è in corso, l'utente ne verrà informato tramite la finestra popup sulla barra delle applicazioni:

Modalità notifica minacce

Nella parte inferiore della finestra di dialogo, scegliere in che modo si desidera essere informati circa eventuali minacce rilevate: mediante una finestra popup standard, mediante una notifica tramite fumetto nella barra delle applicazioni oppure mediante le informazioni dell'icona nella barra delle applicazioni.

La finestra di dialogo ***Protezione Web*** consente di modificare la configurazione del componente relativamente alla scansione del contenuto di siti Web. L'interfaccia di modifica consente di configurare le seguenti opzioni di base:

- ***Abilita Protezione Web***: questa opzione conferma l'esecuzione della scansione del contenuto delle pagine Web da parte del componente ***Online Shield***. Se questa opzione è attivata (*per impostazione predefinita*), è possibile attivare/disattivare anche questi elementi:
    - ***Controlla archivi*** (*disattivata per impostazione predefinita*): consente di eseguire la scansione del contenuto di eventuali archivi inclusi nella pagina Web da visualizzare.

- ***Segnalazione di programmi potenzialmente indesiderati e minacce spyware*** (*attivata per impostazione predefinita*): selezionare questa casella di controllo per attivare il motore Anti-Spyware ed eseguire la scansione per ricercare spyware e virus. Gli spyware rappresentano una categoria di malware anomala: anche se solitamente costituiscono un rischio per la sicurezza, alcuni di questi programmi possono essere installati intenzionalmente. Si consiglia di mantenere questa funzionalità attivata in quanto consente di aumentare la protezione del computer.

- ***Segnala set potenziati di programmi potenzialmente indesiderati***: (*disattivata per impostazione predefinita*) selezionare questa casella di controllo per rilevare pacchetti estesi di spyware, ovvero programmi perfettamente normali e innocui al momento dell'acquisto diretto presso il produttore, ma utilizzabili a scopi dannosi successivamente. Si tratta di una precauzione aggiuntiva che aumenta ulteriormente la protezione del computer, ma che potrebbe bloccare programmi legittimi, pertanto l'opzione è disattivata per impostazione predefinita.

- ***Usa analisi euristica***: (*attivata per impostazione predefinita*) consente di eseguire la scansione del contenuto della pagina da visualizzare utilizzando il metodo dell'analisi euristica (*emulazione dinamica delle istruzioni dell'oggetto sottoposto a scansione in un ambiente informatico virtuale*).

- ***Attiva scansione completa*** (*disattivata per impostazione predefinita*): in situazioni specifiche (*se si sospetta che il computer sia stato infettato*) per maggiore sicurezza è possibile selezionare questa opzione per attivare gli algoritmi di scansione più completi che esamineranno anche le aree del computer che difficilmente vengono infettate. Tenere presente tuttavia che questo metodo è piuttosto dispendioso in termini di tempo.

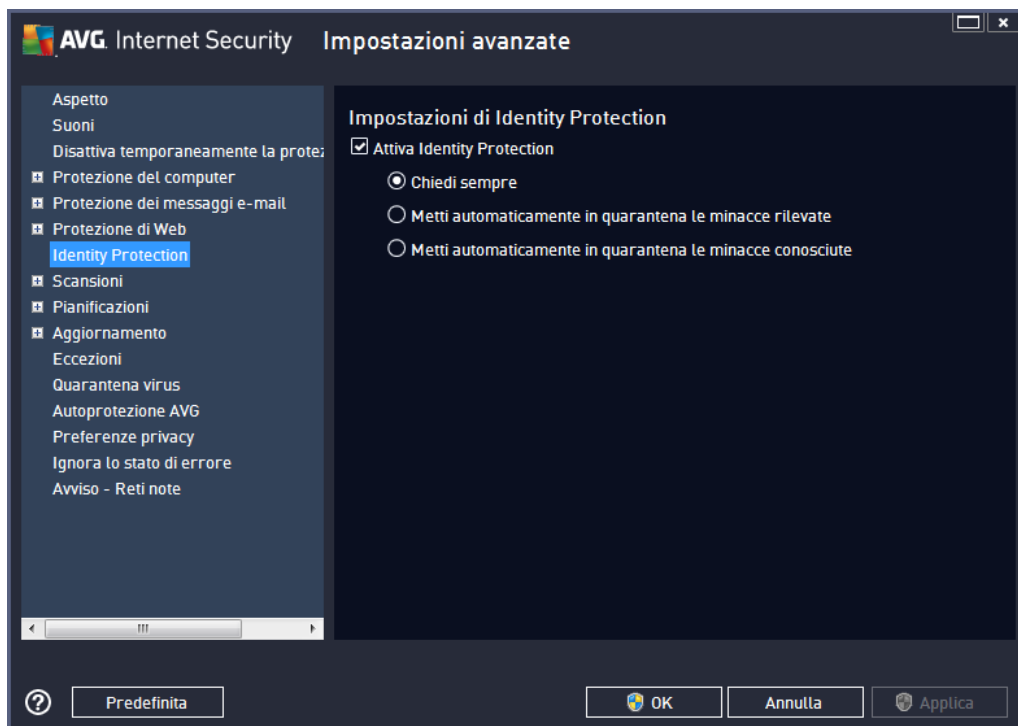
- ***Dimensione massima del file da esaminare***: se i file inclusi sono presenti nella pagina visualizzata, è inoltre possibile eseguire la scansione del relativo contenuto prima che questi vengano scaricati nel computer. Tuttavia, la scansione di file di grandi dimensioni richiede parecchio tempo rallentando notevolmente il download della pagina Web. È possibile utilizzare la barra di scorrimento per specificare la dimensione massima di un file che deve ancora essere sottoposto a scansione da ***Online Shield***. Anche se le dimensioni del file scaricato sono superiori a quelle specificate, e di conseguenza il file non verrà sottoposto a scansione da Online Shield, il computer è comunque protetto: se il file fosse infetto, verrebbe rilevato immediatamente da ***Resident Shield***.

- ***Escludi host/IP/dominio***: nel campo di testo è possibile digitare il nome esatto di un server (*host, indirizzo IP, indirizzo IP con maschera o URL*) o un dominio che non deve essere sottoposto a scansione da ***Online Shield***. Pertanto, escludere un host solo se si è assolutamente certi che non fornirà mai contenuti Web pericolosi.

9.7. Identity Protection

Identity Protection è un componente anti-malware che protegge il computer da qualsiasi tipo di malware (*spyware, bot, furti di identità e così via*) utilizzando tecnologie basate sul comportamento e fornisce la protezione zero day per i nuovi virus *(per una descrizione dettagliata delle funzionalità del componente, vedere il capitolo Identity Protection*).

La finestra di dialogo ***Impostazioni di Identity Protection*** consente di attivare/disattivare le funzioni

di base del componente Identity Protection:

Attiva Identity Protection (*attivata per impostazione predefinita*): deselezionare la casella per disattivare il componente Identity Protection.

Si consiglia di non disattivare questo componente a meno che non sia assolutamente necessario.

Quando Identity Protection è attivato, è possibile specificare l'azione da intraprendere quando viene rilevata una minaccia:

- ***Chiedi sempre***: (*attivata per impostazione predefinita*) quando viene rilevata una minaccia, verrà richiesto se spostarla in quarantena per assicurare che nessuna applicazione da eseguire venga rimossa.

- ***Metti automaticamente in quarantena le minacce rilevate***: selezionare questa casella di controllo per spostare immediatamente tutte le potenziali minacce rilevate nell'area sicura di Quarantena virus. Se si mantengono le impostazioni predefinite, quando una minaccia viene rilevata verrà richiesto se spostarla in quarantena per assicurare che nessuna applicazione da eseguire venga rimossa.

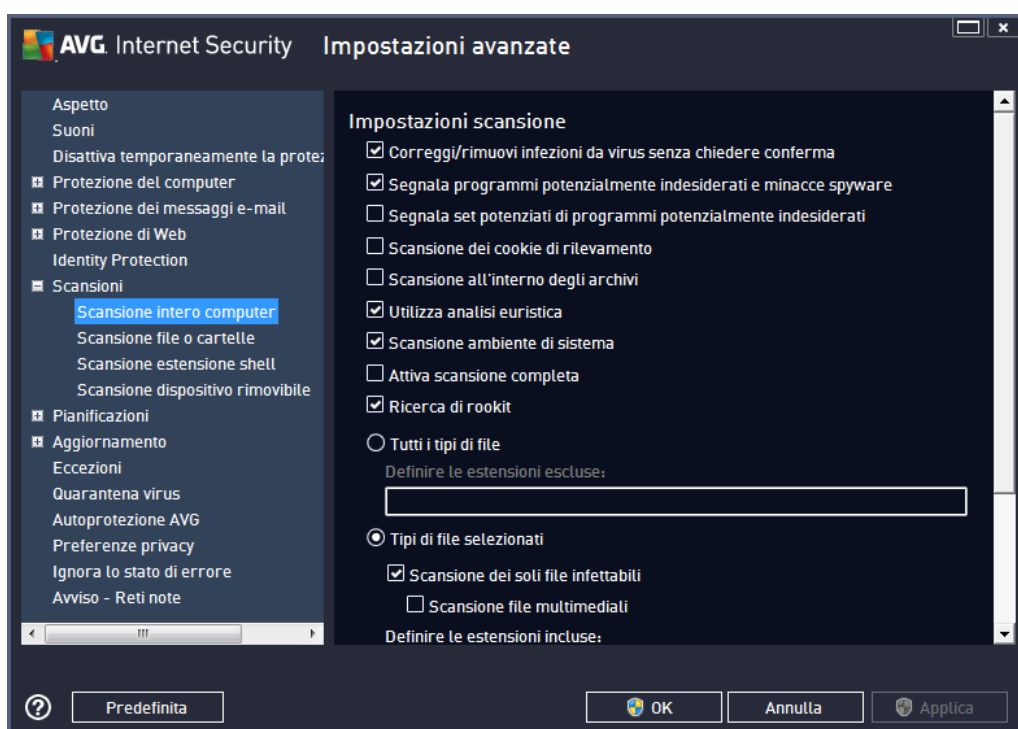
- ***Metti automaticamente in quarantena le minacce conosciute***: mantenere selezionata questa opzione se si desidera che tutte le applicazioni rilevate come possibili malware vengano messe subito in Quarantena virus automaticamente.

9.8. Scansioni

La sezione delle impostazioni di scansione avanzate è suddivisa in quattro categorie che fanno riferimento a specifici tipi di scansione definiti dal fornitore del software:

- ***Scansione intero computer***: scansione predefinita standard dell'intero computer
- ***Scansione estensione shell***: scansione specifica di un oggetto selezionato direttamente dall'ambiente Esplora risorse
- ***Scansione file o cartelle***: scansione predefinita standard di aree selezionate del computer
- ***Scansione dispositivo rimovibile***: scansione specifica di dispositivi rimovibili collegati al computer

9.8.1. Scansione intero computer

L'opzione ***Scansione intero computer*** consente di modificare i parametri di una delle scansioni predefinite dal fornitore del software, ossia Scansione intero computer:

Impostazioni scansione

Nella sezione ***Impostazioni scansione*** è contenuto un elenco di parametri di scansione che possono essere attivati/disattivati a seconda delle necessità:

- ***Correggi/Rimuovi infezioni da virus senza richiedere conferma*** (*attivata per impostazione predefinita*): se viene identificato un virus durante la scansione, può essere corretto automaticamente se è disponibile una soluzione. Se il file infetto non può essere

corretto automaticamente, l'oggetto infetto verrà spostato in Quarantena virus.

- ***Segnala programmi potenzialmente indesiderati e minacce spyware***(*attivata per impostazione predefinita*): selezionare questa casella di controllo per attivare la scansione per ricercare spyware e virus. Gli spyware rappresentano una categoria di malware anomala: anche se solitamente costituiscono un rischio per la sicurezza, alcuni di questi programmi possono essere installati intenzionalmente. Si consiglia di mantenere questa funzionalità attivata in quanto consente di aumentare la protezione del computer.

- ***Segnala set potenziati di programmi potenzialmente indesiderati*** (*disattivata per impostazione predefinita*): selezionare questa casella di controllo per rilevare pacchetti estesi di spyware, ovvero programmi perfettamente normali e innocui al momento dell'acquisto diretto presso il produttore, ma utilizzabili a scopi dannosi successivamente. Si tratta di una precauzione aggiuntiva che aumenta ulteriormente la protezione del computer, ma che potrebbe bloccare programmi legittimi, pertanto l'opzione è disattivata per impostazione predefinita.

- ***Scansione dei cookie di rilevamento*** (*disattivata per impostazione predefinita*): questo parametro specifica che i cookie devono essere rilevati(*i cookie HTTP vengono utilizzati per autenticare, rilevare e mantenere informazioni specifiche sugli utenti, quali le preferenze dei siti o il contenuto dei carrelli elettronici*)

- ***Scansione all'interno degli archivi*** (*disattivata per impostazione predefinita*): questo parametro specifica che la scansione deve controllare tutti i file inclusi all'interno di un archivio, quali ZIP, RAR e così via.

- ***Usa analisi euristiche*** (*attivata per impostazione predefinita*): l'analisi euristica (*emulazione dinamica delle istruzioni dell'oggetto sottoposto a scansione in un ambiente informatico virtuale*) sarà uno dei metodi utilizzati per il rilevamento di virus durante la scansione.

- ***Scansione ambiente di sistema*** (*attivata per impostazione predefinita*): la scansione verrà eseguita anche sulle aree di sistema del computer.

- ***Attiva scansione completa*** (*disattivata per impostazione predefinita*): in situazioni specifiche (*se si sospetta che il computer sia stato infettato*) per maggiore sicurezza è possibile selezionare questa opzione per attivare gli algoritmi di scansione più completi che esamineranno anche le aree del computer che difficilmente vengono infettate. Tenere presente tuttavia che questo metodo è piuttosto dispendioso in termini di tempo.

- ***Ricerca di rootkit*** (*attivata per impostazione predefinita*): la scansione Anti-Rootkit cerca nel computer possibili rootkit, ovvero programmi e tecnologie che possono coprire l'attività dei malware nel computer. Se viene rilevato un rootkit, ciò non significa necessariamente che il computer sia infetto. In alcuni casi, specifici driver o sezioni di applicazioni regolari possono venire rilevati erroneamente come rootkit.

Inoltre, è necessario decidere quali elementi sottoporre a scansione

- ***Tutti i tipi di file***: è possibile definire eccezioni fornendo un elenco di estensioni di file separate da virgola (*dopo il salvataggio, le virgole si trasformano in punto e virgola*) da non sottoporre a scansione;

- ***Tipi di file selezionati***: è possibile specificare che si desidera sottoporre a scansione solo

file potenzialmente infettabili (*i file che non possono essere infettati non verranno sottoposti a scansione, ad esempio alcuni file di testo normale o altri file non eseguibili*), inclusi i file multimediali (*file video e audio, se non si seleziona questa casella, il tempo di scansione risulterà ulteriormente ridotto, poiché questi file sono spesso di grandi dimensioni e non facilmente infettabili dai virus.*). Anche in questo caso, è possibile specificare tramite le estensioni quali file devono essere sempre sottoposti a scansione.

- Facoltativamente, è possibile effettuare la ***Scansione dei file senza estensioni***: questa opzione è attivata per impostazione predefinita e si consiglia di non modificarla a meno che non siano presenti motivi validi per farlo. I file senza estensione sono piuttosto sospetti e devono essere sempre sottoposti a scansione.

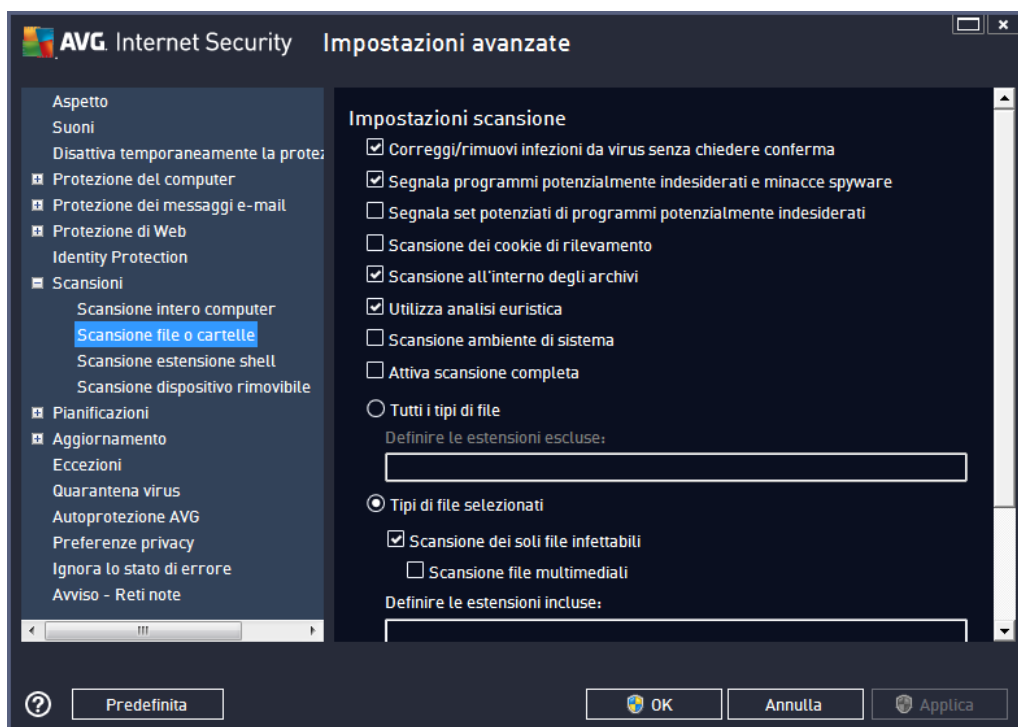
Regola la velocità di completamento della scansione

All'interno della sezione ***Regola la velocità di completamento della scansione*** è inoltre possibile specificare la velocità di scansione desiderata in base all'utilizzo delle risorse di sistema. Per impostazione predefinita, questa opzione è impostata sul livello *sensibile all'utente* per l'utilizzo automatico delle risorse. Se si desidera aumentare la velocità della scansione, il tempo impiegato sarà inferiore ma l'utilizzo delle risorse di sistema aumenterà notevolmente durante l'esecuzione e rallenterà le altre attività svolte sul PC (*questa opzione può essere utilizzata quando il computer è acceso ma non è utilizzato*). Tuttavia, è possibile diminuire l'utilizzo delle risorse di sistema aumentando la durata della scansione.

Imposta rapporti di scansione aggiuntivi...

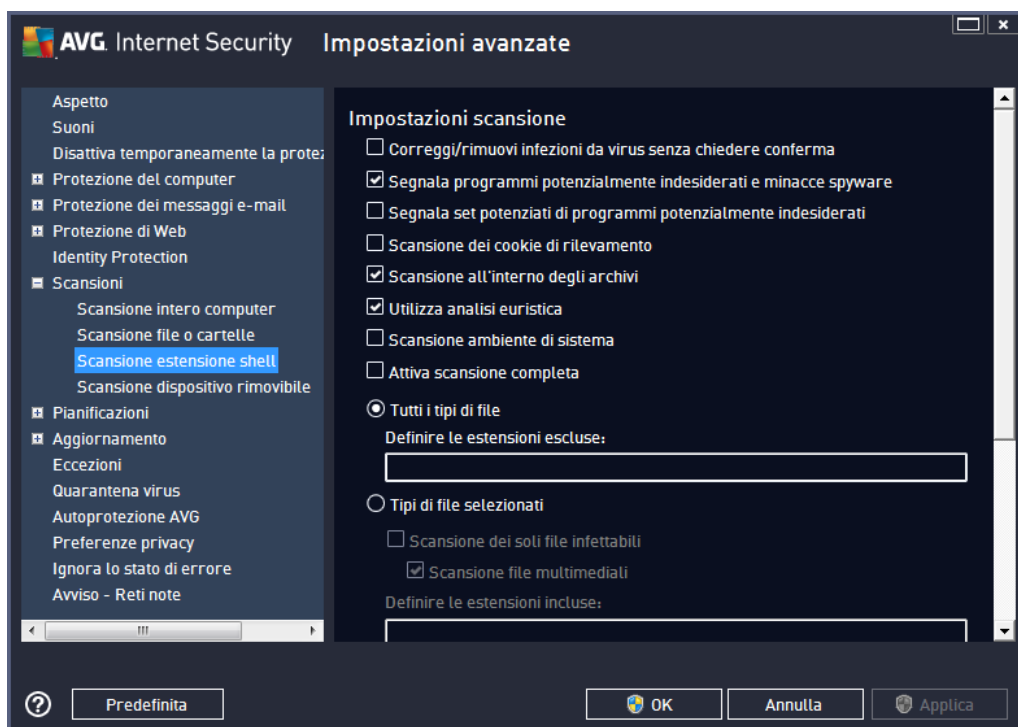
Fare clic sul collegamento ***Imposta rapporti di scansione aggiuntivi...*** per aprire una finestra di dialogo autonoma denominata ***Rapporti di scansione*** in cui è possibile selezionare diversi elementi per definire i tipi di rilevamenti da segnalare:

9.8.2. Scansione file o cartelle

L'interfaccia di modifica di ***Scansione file o cartelle*** è identica alla finestra di dialogo di modifica Scansione intero computer. Tutte le opzioni di configurazione sono uguali; tuttavia, le impostazioni predefinite sono più restrittive per Scansione intero computer:

Tutti i parametri impostati in questa finestra di dialogo di configurazione si applicano solo alle aree selezionate per la scansione con il comando Scansione file o cartelle.

Nota: *per la descrizione di parametri specifici consultare il capitolo Impostazioni AVG avanzate / Scansione / Scansione intero computer.*

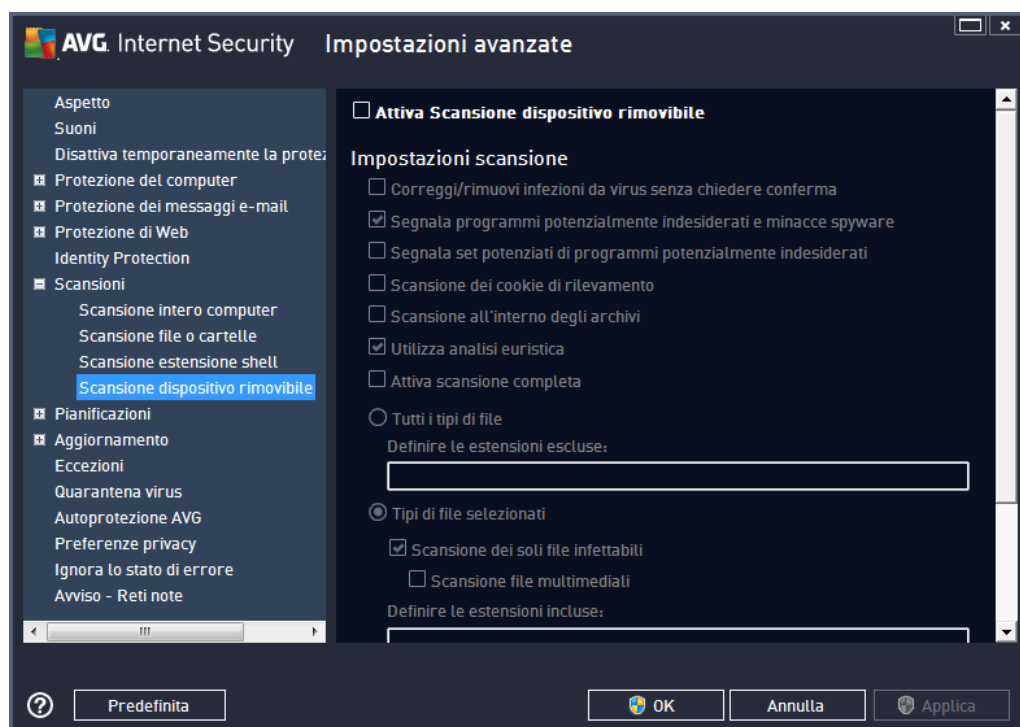
9.8.3. Scansione estensione shell

Simile alla voce precedente denominata Scansione intero computer, ***Scansione estensione shell*** offre anche numerose opzioni per modificare la scansione predefinita dal fornitore del software. In questo caso, la configurazione è correlata alla scansione di oggetti specifici avviati direttamente dall'ambiente Esplora risorse (*estensione shell*), vedere il capitolo Scansione in Esplora risorse:

L'elenco dei parametri è identico a quello disponibile per Scansione intero computer. Tuttavia, le impostazioni predefinite sono diverse (*ad esempio, per impostazione predefinita, Scansione intero computer non controlla gli archivi ma esamina l'ambiente di sistema e viceversa per Scansione estensione shell*).

Nota: *per la descrizione di parametri specifici consultare il capitolo Impostazioni AVG avanzate / Scansione / Scansione intero computer.*

Rispetto alla finestra di dialogo Scansione intero computer, la finestra di dialogo ***Scansione estensione shell*** include inoltre la sezione denominata ***Altre impostazioni correlate all'Interfaccia utente di AVG***, in cui è possibile specificare se si desidera accedere all'avanzamento della scansione e ai risultati della scansione dall'Interfaccia utente di AVG. Inoltre, è possibile definire se il risultato della scansione deve essere visualizzato solo nel caso in cui venga rilevata un'infezione durante la scansione.

9.8.4. Scansione dispositivo rimovibile

L'interfaccia di modifica di ***Scansione dispositivo rimovibile*** è inoltre molto simile alla finestra di dialogo di modifica Scansione intero computer:

La ***Scansione dispositivo rimovibile*** viene avviata automaticamente quando viene collegato un dispositivo rimovibile al computer. Per impostazione predefinita, questa scansione è disattivata. Tuttavia, è molto importante effettuare la scansione dei dispositivi rimovibili per verificare la presenza di potenziali minacce poiché tali dispositivi rappresentano una delle fonti di infezione principali. Per avviare automaticamente questo tipo di scansione quando necessario, selezionare l'opzione ***Abilita scansione dispositivo rimovibile***.

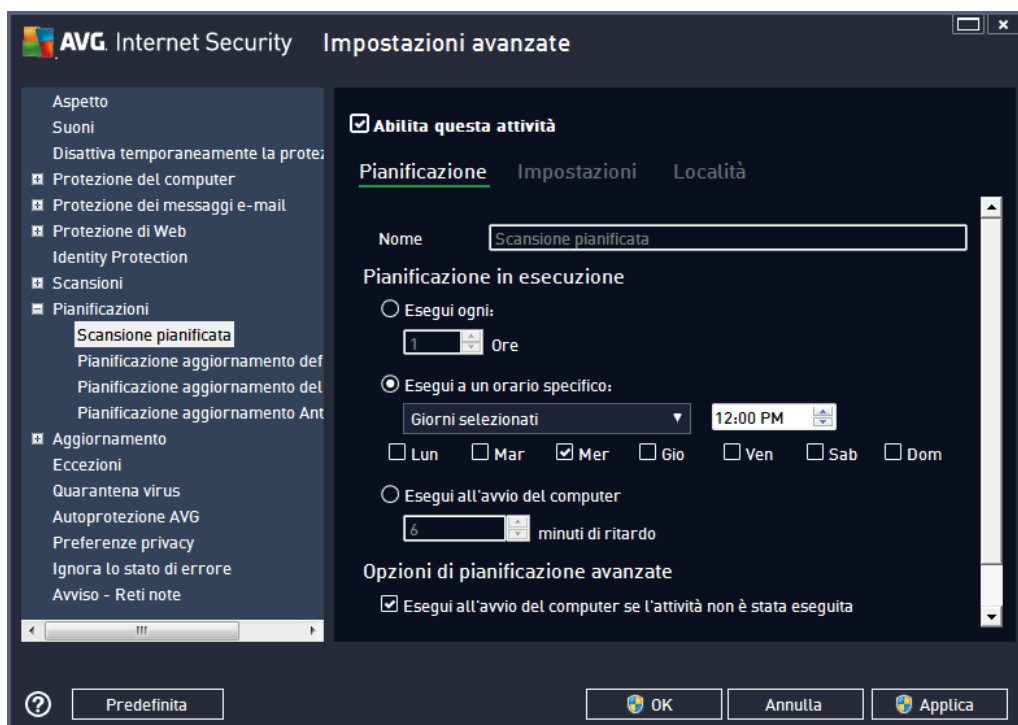
Nota: *per la descrizione di parametri specifici consultare il capitolo Impostazioni AVG avanzate / Scansione / Scansione intero computer.*

9.9. Pianificazioni

Nella sezione ***Pianificazioni*** è possibile modificare le impostazioni predefinite di:

- Scansione pianificata
- Pianificazione aggiornamento definizioni
- Pianificazione aggiornamento del programma
- Pianificazione aggiornamenti Anti-Spam

9.9.1. Scansione pianificata

È possibile modificare i parametri della scansione pianificata (*o impostare una nuova pianificazione*) in tre schede. In ciascuna scheda è possibile selezionare/deselezionare la voce ***Abilita questa attività*** per disattivare temporaneamente il controllo pianificato e riattivarlo secondo le necessità:

Quindi, nel campo di testo ***Nome*** (*disattivato per tutte le pianificazioni predefinite*) è presente il nome assegnato alla pianificazione in oggetto dal fornitore del programma. Per le pianificazioni aggiunte successivamente (*è possibile aggiungere una nuova pianificazione facendo clic con il pulsante destro del mouse sulla voce **Scansione pianificata** nella struttura di esplorazione a sinistra*) è possibile specificare un nome personalizzato. In tal caso, il campo di testo sarà attivo per la modifica. Denominare le scansioni assegnando sempre nomi brevi, descrittivi e appropriati per poterle riconoscere più facilmente in futuro.

Esempio: *non è appropriato denominare una scansione "Nuova scansione" o "Scansione personale" poiché questi nomi non fanno riferimento agli elementi sottoposti a scansione. Un esempio di un buon nome descrittivo potrebbe essere "Scansione aree di sistema" e così via. Inoltre, non è necessario specificare nel nome della scansione se si tratta di una scansione dell'intero computer oppure relativa solo ai file o alle cartelle selezionati. Le scansioni saranno sempre una versione specifica della* *scansione dei file e delle cartelle selezionati*.

In questa finestra di dialogo è possibile definire ulteriormente i seguenti parametri della scansione:

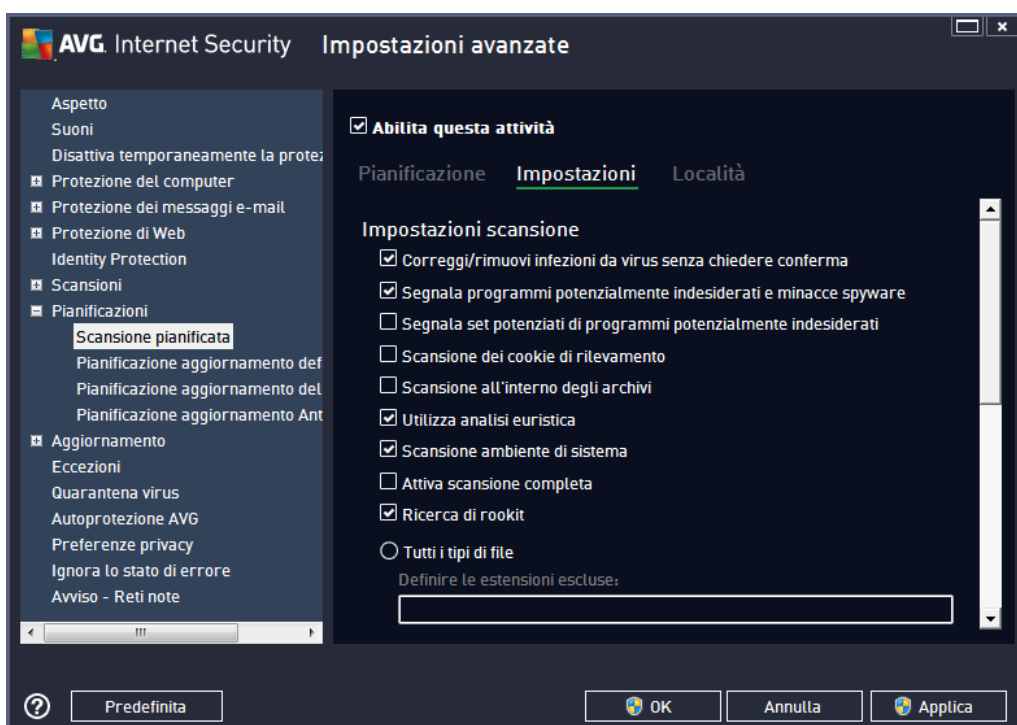
Pianificazione in esecuzione

Consente di specificare gli intervalli di tempo per l'avvio della nuova scansione pianificata. È possibile definire l'ora tramite l'avvio ripetuto della scansione dopo un certo periodo di tempo (***Esegui ogni...***)

oppure specificando data e ora esatte (***Esegui a determinati intervalli di tempo...***) o specificando un evento a cui dovrà essere associato l'avvio della scansione (***Esegui all'avvio del computer***).

Opzioni di pianificazione avanzate

Questa sezione consente di definire le circostanze in cui deve essere avviata o non avviata la scansione se il computer si trova in modalità basso consumo oppure se è completamente spento. Quando la scansione pianificata viene avviata in corrispondenza dell'ora specificata, l'utente ne viene informato tramite una finestra a comparsa visualizzata sopra l'icona di AVG presente nella barra delle applicazioni:

Viene quindi visualizzata una nuova icona AVG nella barra delle applicazioni (*completamente colorata e con una luce lampeggiante*) per comunicare che è in corso una scansione pianificata. Fare clic con il pulsante destro del mouse sull'icona AVG della scansione in esecuzione per aprire un menu di scelta rapida in cui è possibile decidere se sospendere o arrestare la scansione in esecuzione, nonché modificarne la priorità.

Nella scheda ***Impostazioni***è contenuto un elenco di parametri di scansione che possono essere attivati/disattivati facoltativamente. Per impostazione predefinita, la maggior parte dei parametri è attivata e la funzionalità verrà applicata durante la scansione. ***A meno che ci sia una ragione valida per modificare le impostazioni, si consiglia di mantenere la configurazione predefinita***:

- ***Correggi/Rimuovi infezioni da virus senza richiedere conferma*** *(attivata per impostazione predefinita):* se viene identificato un virus durante la scansione, può essere corretto automaticamente se è disponibile una soluzione. Se il file infetto non può essere corretto automaticamente, l'oggetto infetto verrà spostato in Quarantena virus.

- ***Segnala programmi potenzialmente indesiderati e minacce spyware*** *(attivata per impostazione predefinita):* selezionare questa casella di controllo per attivare la scansione per ricercare spyware e virus. Gli spyware rappresentano una categoria di malware anomala: anche se solitamente costituiscono un rischio per la sicurezza, alcuni di questi programmi possono essere installati intenzionalmente. Si consiglia di mantenere questa funzionalità attivata in quanto consente di aumentare la protezione del computer.

- ***Segnala set potenziati di programmi potenzialmente indesiderati*** (*disattivata per impostazione predefinita*): selezionare questa casella di controllo per rilevare pacchetti estesi di spyware, ovvero programmi perfettamente normali e innocui al momento dell'acquisto diretto presso il produttore, ma utilizzabili a scopi dannosi successivamente. Si tratta di una precauzione aggiuntiva che aumenta ulteriormente la protezione del computer, ma che potrebbe bloccare programmi legittimi, pertanto l'opzione è disattivata per impostazione predefinita.

- ***Scansione dei cookie di rilevamento*** (*disattivata per impostazione predefinita*): questo parametro stabilisce che i cookie devono essere rilevati durante la scansione (*i cookie HTTP vengono utilizzati per autenticare, rilevare e mantenere informazioni specifiche sugli utenti, quali le preferenze dei siti o il contenuto dei carrelli elettronici*)

- ***Scansione all'interno degli archivi*** (*disattivata per impostazione predefinita*): questo parametro stabilisce che la scansione deve controllare tutti i file anche se inclusi all'interno di un tipo di archivio, quale ZIP, RAR e così via.

- ***Usa analisi euristiche*** (*attivata per impostazione predefinita*): l'analisi euristica (*emulazione dinamica delle istruzioni dell'oggetto sottoposto a scansione in un ambiente informatico virtuale*) sarà uno dei metodi utilizzati per il rilevamento di virus durante la scansione.

- ***Scansione ambiente di sistema*** (*attivata per impostazione predefinita*): la scansione verrà eseguita anche sulle aree di sistema del computer.

- ***Attiva scansione completa*** (*disattivata per impostazione predefinita):* in situazioni specifiche, *ad esempio se si sospetta che il computer sia stato infettato*, per maggiore sicurezza è possibile selezionare questa opzione per attivare gli algoritmi di scansione più completi che esamineranno anche le aree del computer che difficilmente vengono infettate. Tenere presente tuttavia che questo metodo è piuttosto dispendioso in termini di tempo.

- ***Ricerca di rootkit*** *(attivata per impostazione predefinita):* la scansione Anti-Rootkit cerca nel computer possibili rootkit, ovvero programmi e tecnologie che possono coprire l'attività dei malware nel computer. Se viene rilevato un rootkit, ciò non significa necessariamente che il computer sia infetto. In alcuni casi, specifici driver o sezioni di applicazioni regolari possono venire rilevati erroneamente come rootkit.

Inoltre, è necessario decidere quali elementi sottoporre a scansione

- ***Tutti i tipi di file***: è possibile definire eccezioni fornendo un elenco di estensioni di file separate da virgola (*dopo il salvataggio, le virgole si trasformano in punto e virgola*) da non sottoporre a scansione;

- ***Tipi di file selezionati***: è possibile specificare che si desidera sottoporre a scansione solo file potenzialmente infettabili (*i file che non possono essere infettati non verranno sottoposti a scansione, ad esempio alcuni file di testo normale o altri file non eseguibili*), inclusi i file multimediali (*file video e audio, se non si seleziona questa casella, il tempo di scansione risulterà ulteriormente ridotto, poiché questi file sono spesso di grandi dimensioni e non facilmente infettabili dai virus.*). Anche in questo caso, è possibile specificare tramite le estensioni quali file devono essere sempre sottoposti a scansione.

- Facoltativamente, è possibile effettuare la ***Scansione dei file senza estensioni***: questa opzione è attivata per impostazione predefinita e si consiglia di non modificarla a meno che non siano presenti motivi validi per farlo. I file senza estensione sono piuttosto sospetti e devono essere sempre sottoposti a scansione.

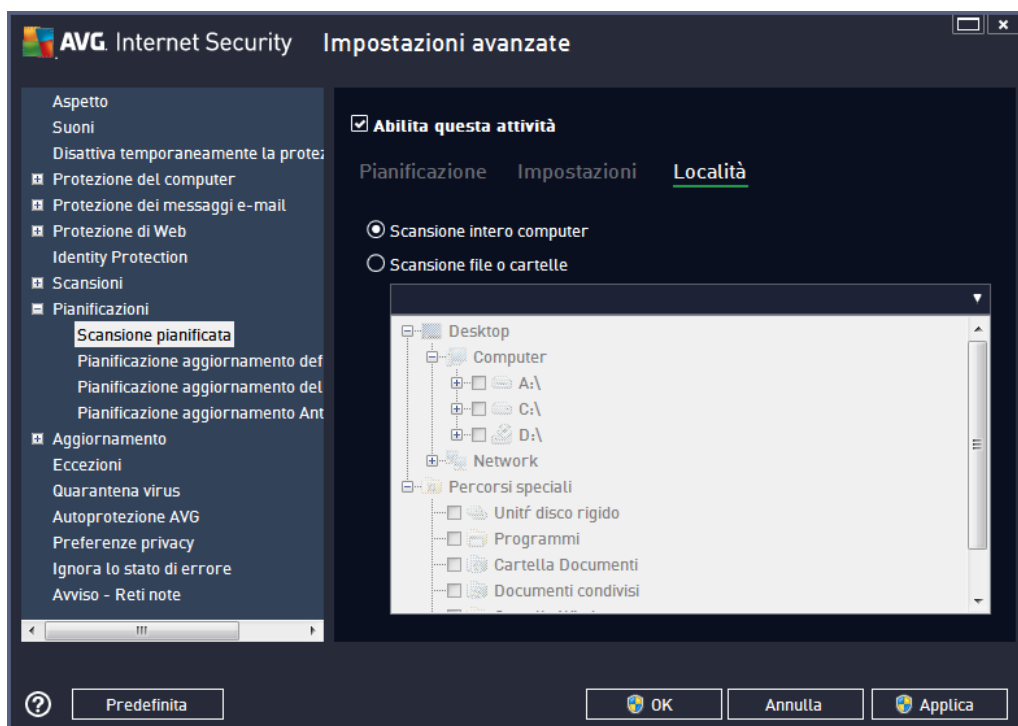
Regola la velocità di completamento della scansione

All'interno di questa sezione è inoltre possibile specificare la velocità di scansione desiderata in base all'utilizzo delle risorse di sistema. Per impostazione predefinita, questa opzione è impostata sul livello *Sensibile all'utente* per l'utilizzo automatico delle risorse. Se si desidera aumentare la velocità della scansione, il tempo impiegato sarà inferiore ma l'utilizzo delle risorse di sistema aumenterà notevolmente durante l'esecuzione e rallenterà le altre attività svolte sul PC (*questa opzione può essere utilizzata quando il computer è acceso ma non è utilizzato*). Tuttavia, è possibile diminuire l'utilizzo delle risorse di sistema aumentando la durata della scansione.

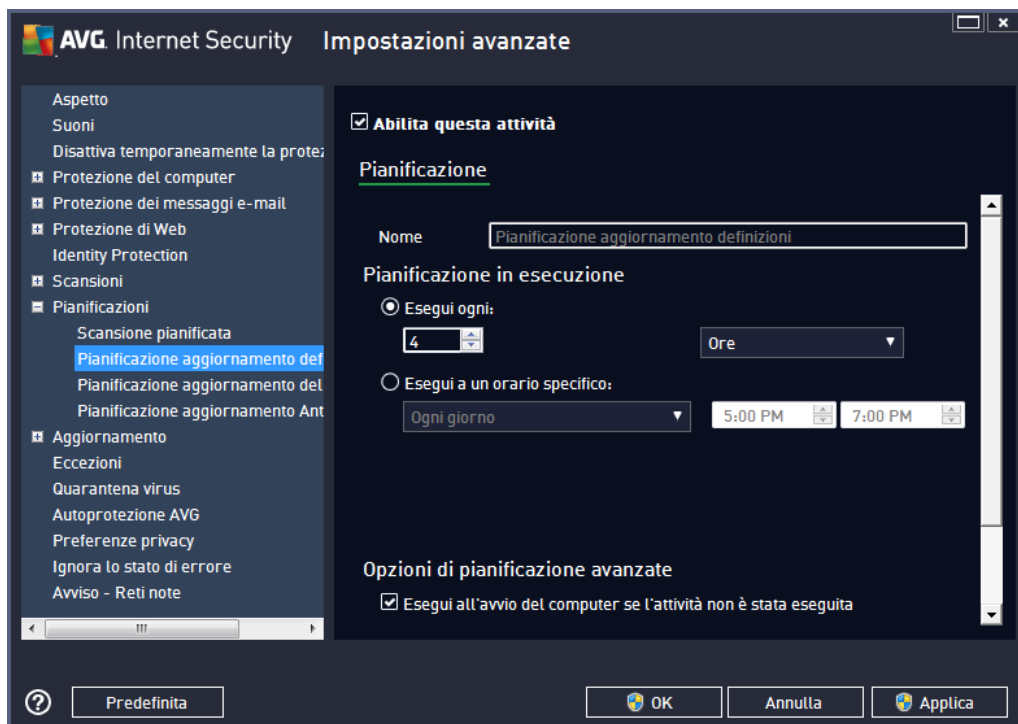
Imposta rapporti di scansione aggiuntivi

Fare clic sul collegamento ***Imposta rapporti di scansione aggiuntivi...*** per aprire una finestra di dialogo autonoma denominata ***Rapporti di scansione*** in cui è possibile selezionare diversi elementi per definire i tipi di rilevamenti da segnalare:

Opzioni arresto computer

Nella sezione ***Opzioni arresto computer***, è possibile decidere se il computer deve essere arrestato in modo automatico al termine del processo di scansione. Dopo aver confermato questa opzione (***Arresta computer al completamento della scansione***), viene attivata una nuova opzione che consente l'arresto del computer anche se è correntemente bloccato (***Forza arresto se il computer è bloccato***).

Nella scheda ***Posizione*** è possibile definire se si desidera pianificare la scansione dell'intero computer o la scansione di file o cartelle. Se si seleziona la scansione di file o cartelle, nella parte inferiore di questa finestra di dialogo viene attivata la struttura visualizzata che consente di specificare le cartelle da sottoporre a scansione.

9.9.2. Pianificazione aggiornamento definizioni

Se ***realmente necessario***, è possibile deselezionare la voce ***Abilita questa attività*** per disattivare temporaneamente l'aggiornamento delle definizioni pianificato e attivarlo nuovamente in seguito:

In questa finestra di dialogo è possibile impostare alcuni parametri dettagliati della pianificazione dell'aggiornamento delle definizioni. Nel campo di testo ***Nome*** (*disattivato per tutte le pianificazioni predefinite*) è presente il nome assegnato alla pianificazione in oggetto dal fornitore del programma.

Pianificazione in esecuzione

In questa sezione, specificare gli intervalli di tempo per l'avvio del nuovo aggiornamento delle definizioni pianificato. L'intervallo può essere definito tramite l'avvio dell'aggiornamento ripetuto dopo un determinato periodo di tempo (***Esegui ogni...***) oppure specificando una data e un'ora esatte (***Esegui a un orario specifico...***).

Opzioni di pianificazione avanzate

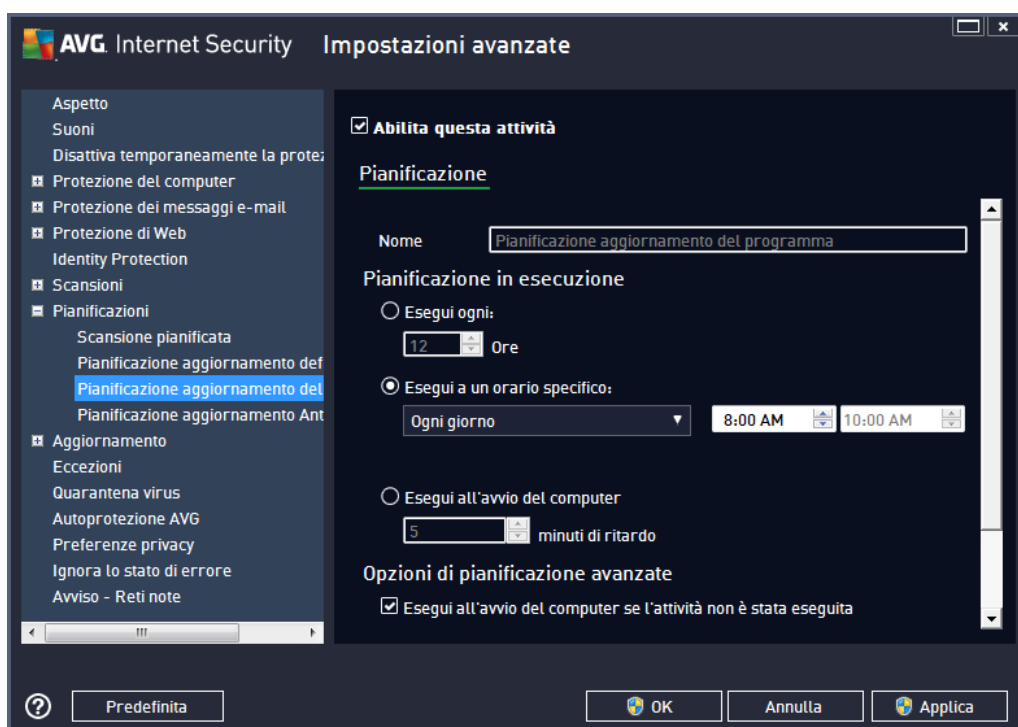
Questa sezione consente di definire le circostanze in cui deve essere avviato o non avviato l'aggiornamento se il computer si trova in modalità basso consumo oppure se è completamente spento.

Altre impostazioni di aggiornamento

Infine, selezionare l'opzione ***Eseguire nuovamente l'aggiornamento quando la connessione Internet sarà disponibile*** per assicurarsi che, se la connessione Internet si interrompesse e il

processo di aggiornamento non riuscisse, tale processo venga avviato di nuovo subito dopo il ripristino della connessione Internet. Quando l'aggiornamento pianificato viene avviato in corrispondenza dell'ora specificata, l'utente ne viene informato tramite una finestra popup visualizzata sopra l'icona nella barra delle applicazioni di AVG (*a condizione che sia stata mantenuta la configurazione predefinita della finestra di dialogo Impostazioni avanzate/Aspetto*).

9.9.3. Pianificazione dell'aggiornamento del programma

Se ***realmente necessario***, è possibile deselezionare la voce ***Abilita questa attività*** per disattivare temporaneamente l'aggiornamento del programma pianificato e attivarlo nuovamente in seguito:

Nel campo di testo ***Nome*** (*disattivato per tutte le pianificazioni predefinite*) è presente il nome assegnato alla pianificazione in oggetto dal fornitore del programma.

Pianificazione in esecuzione

Consente di specificare gli intervalli di tempo per l'avvio del nuovo aggiornamento del programma pianificato. È possibile definire l'ora tramite l'avvio ripetuto dell'aggiornamento dopo un certo periodo di tempo (***Esegui ogni...***) oppure definendo data e ora esatte (***Esegui a un orario specifico...***) o definendo un evento a cui dovrà essere associato l'avvio dell'aggiornamento (***Azione in base all'avvio del computer***).

Opzioni di pianificazione avanzate

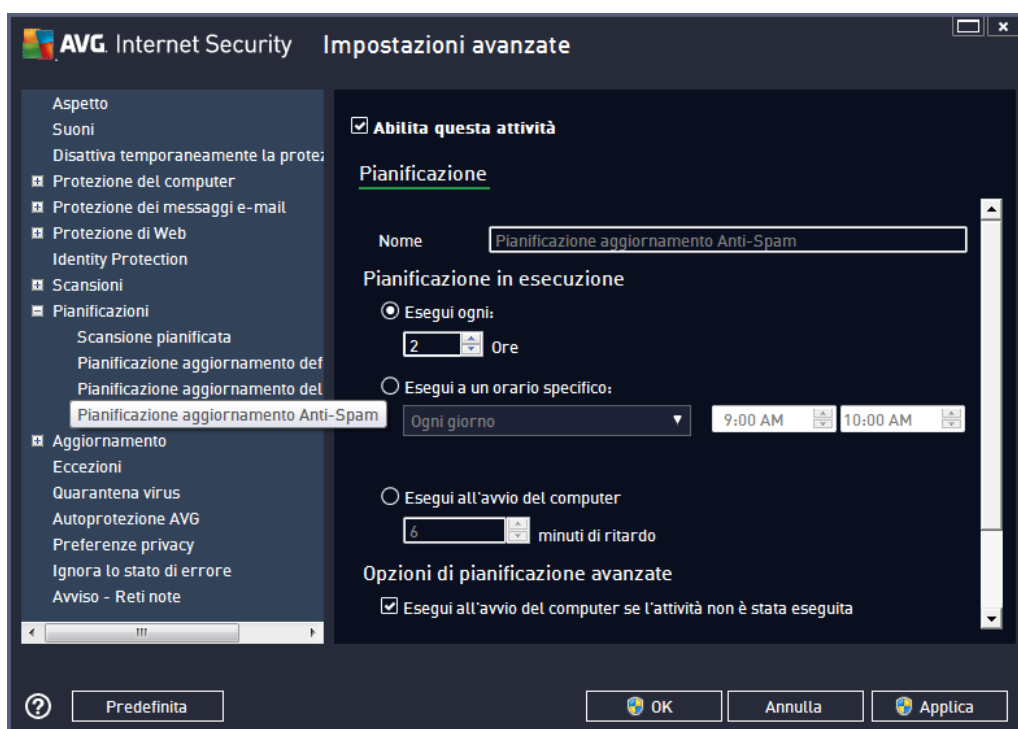
Questa sezione consente di definire le circostanze in cui deve o non deve essere avviato l' aggiornamento del programma se il computer si trova in modalità basso consumo oppure se è completamente spento.

Altre impostazioni per l'aggiornamento

Selezionare l'opzione ***Eseguire nuovamente l'aggiornamento quando la connessione Internet sarà disponibile*** per assicurarsi che, se la connessione Internet si interrompesse e il processo di aggiornamento non riuscisse, tale processo venga avviato di nuovo subito dopo il ripristino della connessione Internet. Quando l'aggiornamento pianificato viene avviato in corrispondenza dell'ora specificata, l'utente ne viene informato tramite una finestra popup visualizzata sopra l'icona della barra delle applicazioni di AVG (*a condizione che sia stata mantenuta la configurazione predefinita della finestra di dialogo Impostazioni avanzate/Aspetto*).

Nota: *se gli orari di un aggiornamento del programma pianificato e di una scansione pianificata dovessero coincidere, il processo di aggiornamento acquista priorità e la scansione viene interrotta.*

9.9.4. Pianificazione aggiornamenti Anti-Spam

Se realmente necessario, è possibile deselezionare la voce ***Abilita questa attività*** per disattivare temporaneamente l'aggiornamento Anti-Spam pianificato e attivarlo nuovamente in seguito:

In questa finestra di dialogo è possibile impostare alcuni parametri dettagliati per la pianificazione dell'aggiornamento. Il campo di testo ***Nome*** (*disattivato per tutte le pianificazioni predefinite*) indica il nome assegnato alla pianificazione in oggetto dal fornitore del programma.

Pianificazione in esecuzione

Questa sezione consente di specificare gli intervalli di tempo per l'avvio dell'aggiornamento Anti-Spam che è stato pianificato. È possibile specificare l'ora dall'avvio ripetuto dell'aggiornamento Anti-Spam dopo un certo periodo di tempo (***Esegui ogni***) o definendo data e ora esatte (***Esegui a un***

orario specifico) oppure definendo un evento a cui dovrà essere associato l'avvio dell'aggiornamento (***Esegui all'avvio del computer***).

Opzioni di pianificazione avanzate

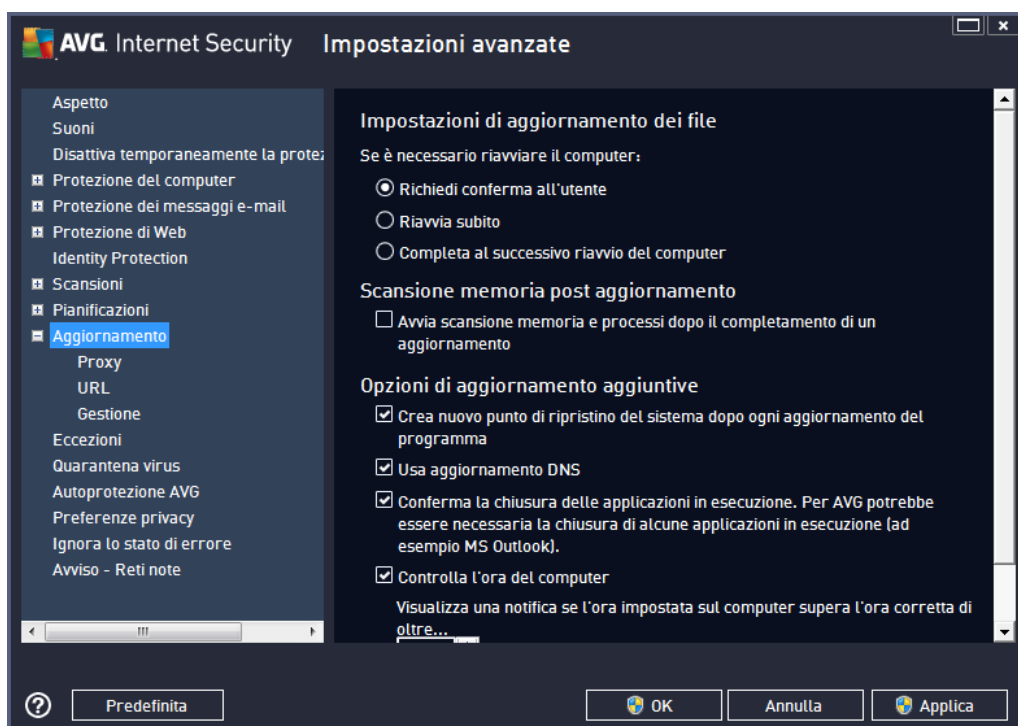
Questa sezione consente di definire le circostanze in cui deve essere avviato o non avviato l'aggiornamento Anti-Spam se il computer si trova in modalità basso consumo oppure se è completamente spento.

Altre impostazioni di aggiornamento

Selezionare l'opzione ***Eseguire nuovamente l'aggiornamento quando la connessione Internet sarà disponibile*** per assicurarsi che, se la connessione Internet si interrompesse e il processo di aggiornamento Anti-Spam non riuscisse, tale processo venga avviato di nuovo subito dopo il ripristino della connessione Internet.

Quando la scansione pianificata viene avviata in corrispondenza dell'ora specificata, l'utente ne viene informato tramite una finestra popup visualizzata sopra l'icona nella barra delle applicazioni di AVG (*a condizione che sia stata mantenuta la configurazione predefinita della finestra di dialogo Impostazioni avanzate/Aspetto*).

9.10. Aggiornamento

La voce ***Aggiorna*** consente di aprire una finestra di dialogo in cui è possibile specificare i parametri generali relativi all'aggiornamento di AVG:

Quando eseguire l'aggiornamento dei file

In questa sezione è possibile effettuare la selezione tra tre diverse opzioni da utilizzare nel caso in cui il processo di aggiornamento richieda il riavvio del PC. È possibile pianificare la finalizzazione dell'aggiornamento per il successivo riavvio del PC oppure è possibile procedere subito al riavvio:

- ***Richiedi conferma dell'utente*** *(impostazione predefinita)*: verrà richiesto di approvare un riavvio del PC necessario per finalizzare il processo di aggiornamento
- ***Riavvia subito***: il computer verrà riavviato immediatamente in maniera automatica dopo la finalizzazione del processo di aggiornamento senza richiesta di conferma da parte dell'utente
- ***Completa al successivo riavvio del computer***: la finalizzazione del processo di aggiornamento verrà posticipata al successivo riavvio del computer. Tenere presente che questa opzione è consigliata solo se si è certi che il computer venga riavviato regolarmente, almeno una volta al giorno.

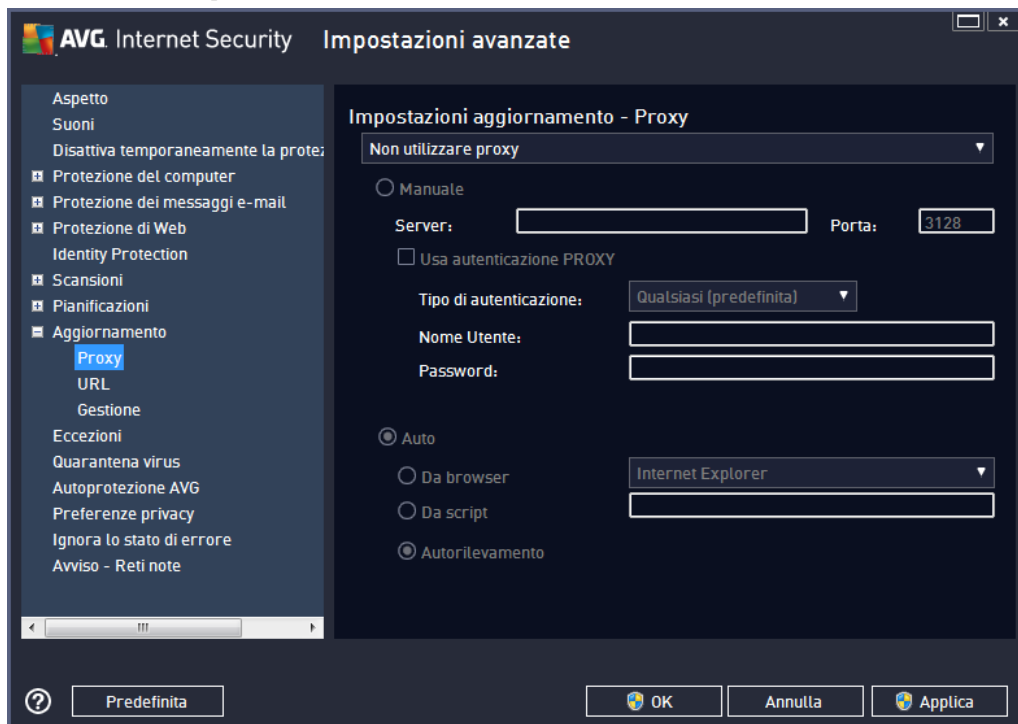
Scansione memoria post aggiornamento

Selezionare questa casella di controllo per specificare che si desidera avviare una nuova scansione della memoria al termine di ciascun aggiornamento. L'ultimo aggiornamento scaricato potrebbe contenere nuove definizioni dei virus e queste potrebbero applicarsi immediatamente alla scansione.

Opzioni di aggiornamento aggiuntive

- ***Crea nuovo punto di ripristino del sistema durante ogni aggiornamento del programma***: prima dell'avvio di ciascun aggiornamento del programma AVG viene creato un punto di ripristino del sistema. Se il processo di aggiornamento non ha esito positivo e il sistema operativo si blocca, è possibile ripristinare il sistema operativo nella configurazione originale da questo punto. Questa opzione è accessibile tramite Start / Tutti i programmi / Accessori / Utilità di sistema / Ripristino configurazione di sistema, tuttavia le eventuali modifiche sono consigliate ai soli utenti esperti. Mantenere selezionata questa casella di controllo se si desidera utilizzare questa funzionalità.
- ***Usa aggiornamento DNS*** (*attivata per impostazione predefinita*): con questa voce selezionata, una volta avviato l'aggiornamento, **AVG Internet Security 2013** ricerca informazioni sulla versione del database dei virus più recente e sulla versione del programma più recente sul server DNS. Quindi, solo i file di aggiornamento più piccoli e indispensabili vengono scaricati e applicati. In questo modo la quantità totale di dati scaricati viene ridotta al minimo e il processo di aggiornamento viene accelerato.
- ***Conferma la chiusura delle applicazioni in esecuzione*** (*attivata per impostazione predefinita*): questa opzione garantirà che nessuna applicazione in esecuzione venga chiusa senza autorizzazione, nel caso fosse necessario per la finalizzazione del processo di aggiornamento.
- ***Controlla l'ora del computer***: selezionare questa opzione per ricevere una notifica nel caso in cui l'ora del computer differisca dall'ora esatta di un valore superiore al numero di

ore specificato.

9.10.1. Proxy

Il server proxy è un server autonomo o un servizio in esecuzione su un PC che garantisce una connessione più sicura a Internet. Secondo le regole di rete specificate è possibile accedere a Internet direttamente o tramite il server proxy. Sono anche consentite entrambe le possibilità contemporaneamente. Quindi, nella prima voce della finestra di dialogo ***Impostazioni aggiornamento – Proxy*** è necessario selezionare l'opzione desiderata dal menu della casella combinata:

- ***Non utilizzare proxy***: impostazioni predefinite
- ***Utilizza proxy***
- ***Tenta la connessione utilizzando il proxy e, se non riesce, esegui la connessione direttamente***

Se si seleziona un'opzione utilizzando un server proxy, sarà necessario specificare ulteriori dati. Le impostazioni del server possono essere configurate manualmente o automaticamente.

Configurazione manuale

Se si seleziona la configurazione manuale (selezionare *l'opzione* ***Manuale*** *per attivare la sezione della finestra di dialogo corrispondente*) è necessario specificare le seguenti voci:

- ***Server***: specificare l'indirizzo IP o il nome del server

- ***Porta***: specifica il numero della porta che consente l'accesso a Internet (*per impostazione predefinita, il numero è impostato su 3128 ma può essere modificato – se non si è sicuri, contattare l'amministratore di rete*)

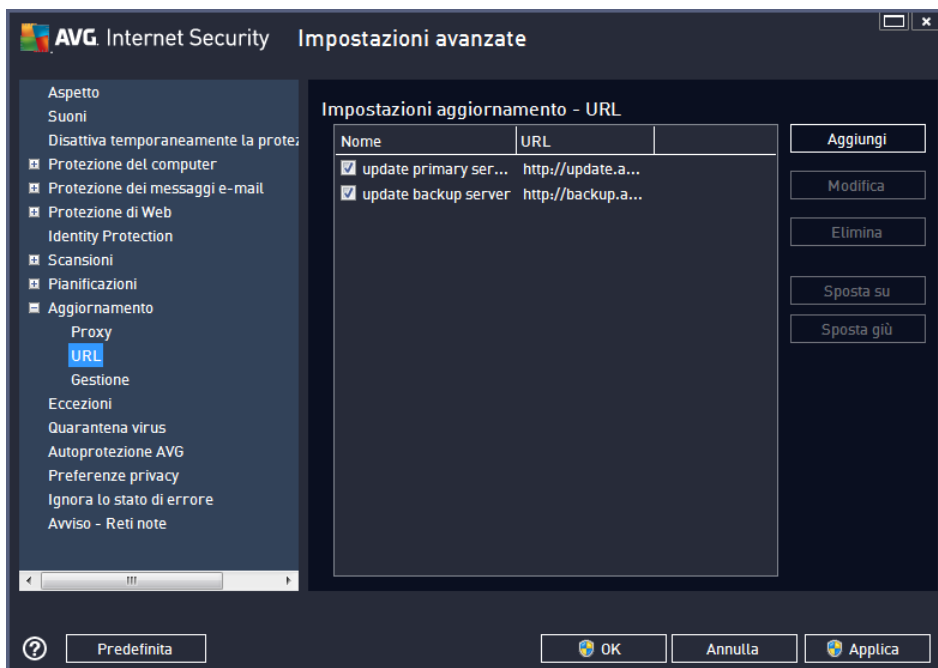
È anche possibile che sul server proxy siano state configurate regole specifiche per ciascun utente. Se il server proxy è impostato in questo modo, selezionare l'opzione ***Usa autenticazione PROXY*** per verificare che nome utente e password siano validi per la connessione a Internet tramite il server proxy.

Configurazione automatica

Se si seleziona la configurazione automatica *(selezionare l'opzione **Auto** per attivare la sezione della finestra di dialogo corrispondente*), selezionare quindi l'origine della configurazione proxy:

- ***Da browser***: la configurazione verrà letta dal browser Internet predefinito
- ***Da script***: la configurazione verrà letta da uno script scaricato con la funzione di restituzione dell'indirizzo proxy
- ***Autorilevamento***: la configurazione verrà rilevata automaticamente direttamente dal server proxy

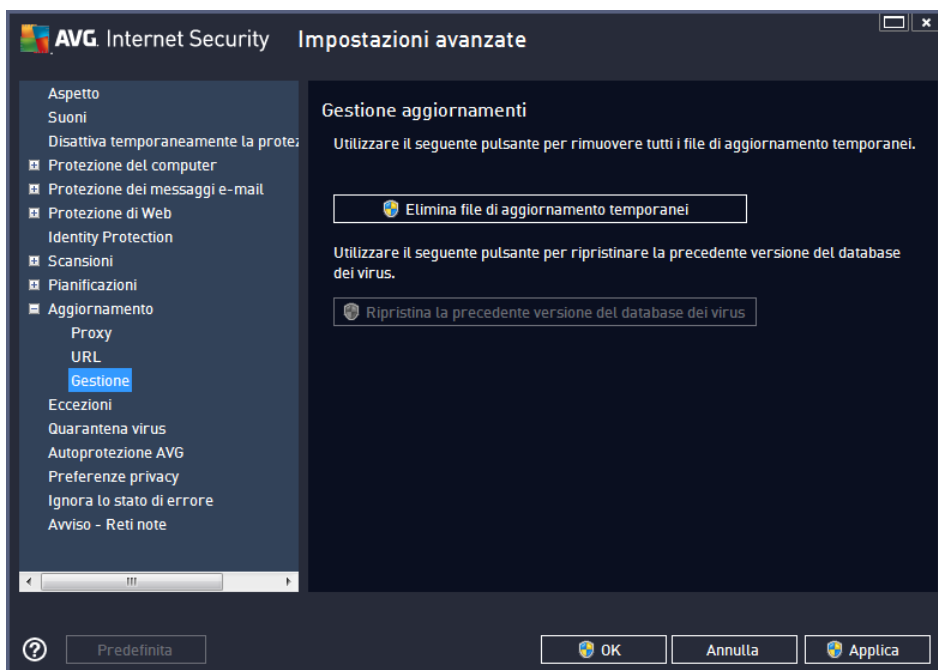
9.10.2. URL

Nella finestra di dialogo ***URL*** è contenuto un elenco di indirizzi Internet da cui è possibile scaricare i file di aggiornamento:

Pulsanti di controllo

È possibile modificare l'elenco e i suoi elementi utilizzando i seguenti pulsanti di controllo:

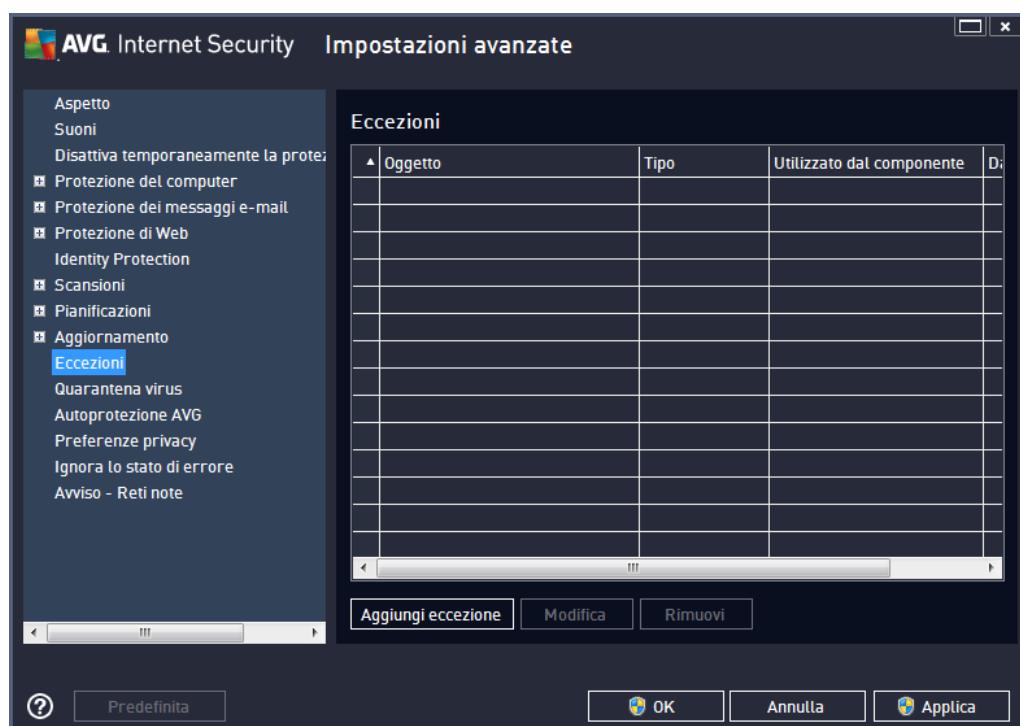
- ***Aggiungi*** :consente di aprire una finestra di dialogo in cui è possibile specificare un nuovo URL da aggiungere all'elenco
- ***Modifica***: consente di aprire una finestra di dialogo in cui è possibile modificare i parametri dell'URL selezionato
- ***Elimina***: consente di eliminare l'URL selezionato dall'elenco
- ***Sposta Su***: consente di spostare l'URL selezionato di una posizione verso l'alto nell'elenco
- ***Sposta Giù***: consente di spostare l'URL selezionato di una posizione verso il basso nell'elenco

9.10.3. Gestione

La finestra di dialogo ***Gestione aggiornamenti*** offre due opzioni accessibili tramite due pulsanti:

- ***Elimina file di aggiornamento temporanei***: selezionare questo pulsante per eliminare tutti i file di aggiornamento ridondanti dal disco rigido (*per impostazione predefinita, questi file restano memorizzati per 30 giorni*)
- ***Ripristina la precedente versione del database dei virus***: selezionare questo pulsante per eliminare l'ultima versione del database dei virus dal disco rigido e tornare alla precedente versione salvata (*la nuova versione del database dei virus verrà inserita nel successivo aggiornamento*)

9.11. Eccezioni

Nella finestra di dialogo ***Eccezioni*** è possibile definire le eccezioni, ovvero, voci che **AVG Internet Security 2013** ignorerà. In genere, sarà necessario definire un'eccezione se AVG continua a rilevare un programma o un file come se fosse una minaccia oppure blocca un sito Web sicuro come se fosse pericoloso. Se si aggiungono tali file o siti Web a questo elenco eccezioni, AVG non li segnalerà né bloccherà più.

Assicurasi sempre che il file, il programma o il sito Web in questione sia davvero completamente sicuro.

Nel grafico della finestra di dialogo viene visualizzato un elenco di eccezioni, se sono già state definite. Accanto a ogni elemento è presente una casella di controllo. Se la casella di controllo è selezionata, l'eccezione è attiva. In caso contrario, è semplicemente definita ma non utilizzata. Facendo clic su un'intestazione di colonna, è possibile ordinare gli elementi consentiti in base al criterio corrispondente.

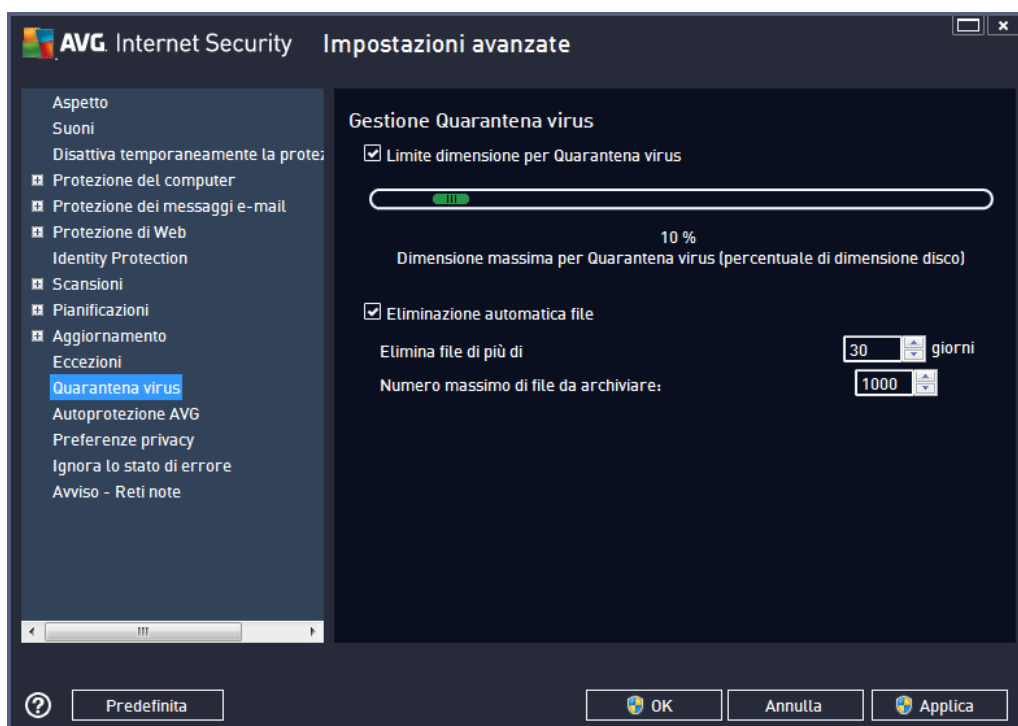
Pulsanti di controllo

- ***Aggiungi eccezione***: fare clic per aprire una nuova finestra di dialogo in cui è possibile specificare la voce che deve essere esclusa dalla scansione AVG. Prima di tutto, verrà richiesto di definire il tipo di oggetto, ovvero se si tratta di un file, una cartella o un URL. Quindi sarà necessario specificare il percorso del relativo oggetto nel disco o digitare l'URL. Infine, è possibile selezionare quali funzionalità AVG devono ignorare l'oggetto selezionato *(Resident Shield, Identity, Scansione, Anti-Rootkit)*.

- ***Modifica***: questo pulsante è attivo solo se alcune eccezioni sono state già definite e inserite nell'elenco. È quindi possibile utilizzare il pulsante per aprire la finestra di modifica

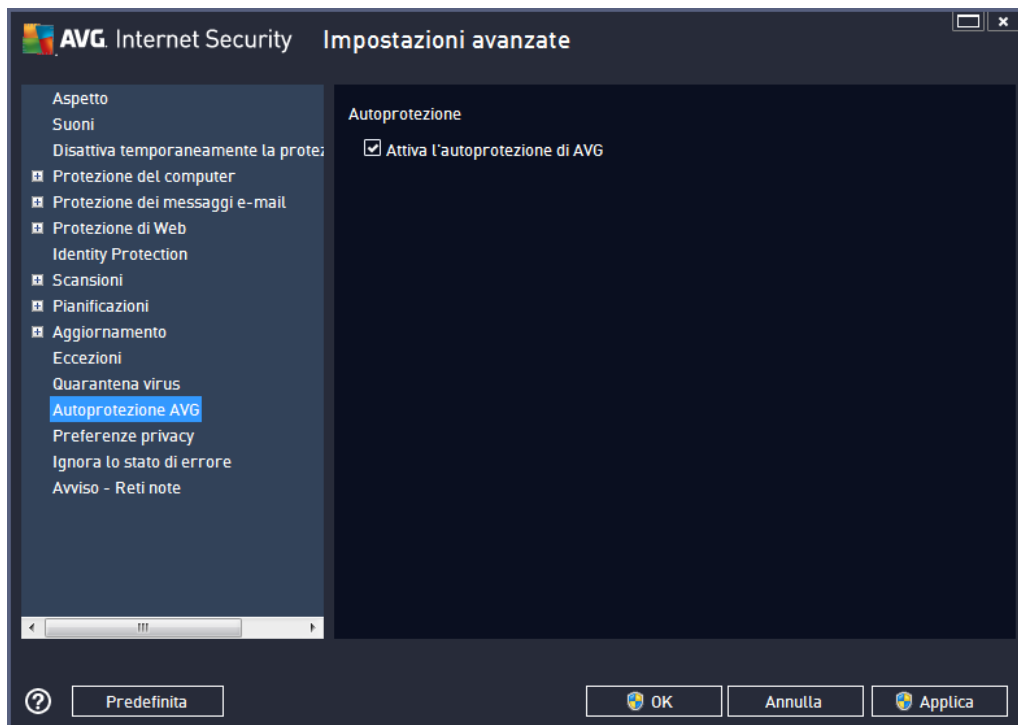
relativa all'eccezione selezionata e configurare i parametri dell'eccezione.

- ***Rimuovi***: questo pulsante consente di annullare un'eccezione definita in precedenza. È possibile rimuovere le eccezioni una per una o evidenziare un blocco nell'elenco e annullare le eccezioni definite. Dopo aver annullato l'eccezione, il file, la cartella o l'URL relativi verranno controllati di nuovo da AVG. Tenere presente che verrà rimossa solo l'eccezione, non il relativo file o cartella!

9.12. Quarantena virus

La finestra di dialogo ***Gestione Quarantena virus*** consente di definire diversi parametri relativi alla gestione degli oggetti archiviati in Quarantena virus:

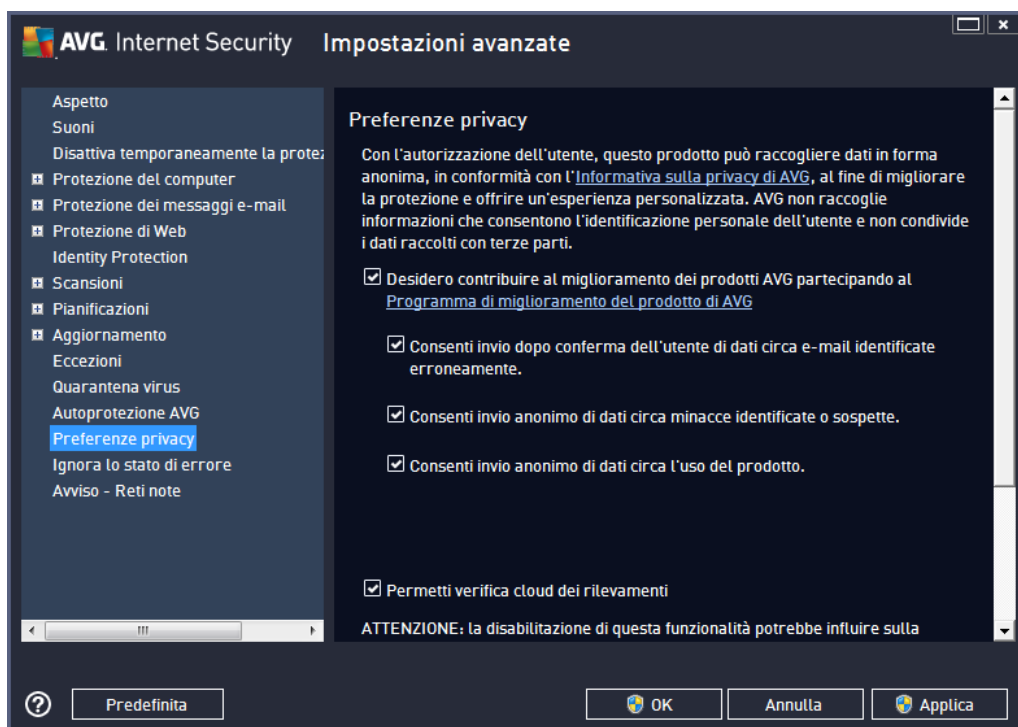
- ***Limite dimensione per Quarantena virus***: utilizzare il dispositivo di scorrimento per impostare la dimensione massima di Quarantena virus. La dimensione è specificata in maniera proporzionale rispetto alla dimensione del disco locale.

- ***Eliminazione automatica file***: questa sezione consente di definire la durata massima di memorizzazione degli oggetti in Quarantena virus (***Elimina file di più di...giorni***) e il numero massimo di file da memorizzare in Quarantena virus (***Numero massimo di file da memorizzare***).

9.13. Autoprotezione di AVG

Autoprotezione di AVG consente a **AVG Internet Security 2013** di proteggere i relativi processi, file, chiavi di registro e driver da modifiche o disattivazioni. Il motivo principale per cui si utilizza questo tipo di protezione è che alcune minacce sofisticate tentano di disattivare la protezione anti-virus per causare liberamente danni al computer.

Si consiglia di mantenere questa funzionalità attivata!

9.14. Preferenze privacy

La finestra di dialogo ***Preferenze privacy*** invita l'utente a partecipare al programma per il miglioramento del prodotto AVG per aiutarci ad aumentare il livello di protezione generale in Internet. La segnalazione ci consente di raccogliere informazioni aggiornate sulle minacce più recenti da tutti gli utenti a livello mondiale e di migliorare la protezione per tutti. La segnalazione viene elaborata automaticamente, pertanto non provoca alcun disturbo all'utente. Nei rapporti non vengono inclusi dati personali. La segnalazione delle minacce rilevate è opzionale. Tuttavia si consiglia si mantenere attivata questa opzione. La segnalazione ci aiuta a migliorare la protezione per tutti gli utenti AVG.

Nella finestra di dialogo sono disponibili le seguenti opzioni di impostazione:

- ***Desidero contribuire al miglioramento dei prodotti AVG partecipando al Programma di miglioramento del prodotto AVG*** *(attivata per impostazione predefinita)*: per aiutarci a migliorare ulteriormente **AVG Internet Security 2013**, mantenere selezionata questa casella di controllo. Ciò consentirà di segnalare ad AVG tutte le minacce riscontrate. In questo modo saremo in grado di raccogliere informazioni aggiornate sui malware da tutti gli utenti a livello mondiale per offrire un livello di protezione ancora superiore. La segnalazione viene elaborata automaticamente, pertanto non provoca alcun disturbo all'utente e nei rapporti non vengono inclusi dati personali.

    - ***Consenti invio dopo conferma dell'utente di dati circa e-mail identificate erroneamente*** *(attivata per impostazione predefinita)*: invia informazioni sui messaggi e-mail identificati erroneamente come spam o sui messaggi di spam non rilevati dal servizio Anti-Spam. Per l'invio di questo tipo di informazioni verrà richiesta la conferma dell'utente.

    - ***Consenti invio anonimo di dati circa minacce identificate o sospette*** *(attiva per impostazione predefinita)*: invia informazioni su comportamenti o codici certamente pericolosi o sospetti *(può trattarsi di un virus, uno spyware o una pagina Web dannosa a cui si sta tentando di accedere) rilevati nel computer.*

    - ***Consenti invio anonimo di dati circa l'uso del prodotto*** *(attiva per impostazione predefinita)* : invia statistiche di base sull'uso dell'applicazione, ad esempio numero di rilevamenti, scansioni avviate, aggiornamenti riusciti/non riusciti e così via.

- ***Permetti verifica cloud dei rilevamenti*** *(attiva per impostazione predefinita)*: le minacce rilevate verranno controllate per verificare l'effettiva presenza di infezioni, in modo da evitare i falsi positivi.

Minacce Web più diffuse

Attualmente le minacce esistenti non si limitano più ai semplici virus. Gli autori di codici dannosi e di siti Web pericolosi hanno molta inventiva, per cui emergono abbastanza di frequente nuovi tipi di minacce, la maggior parte delle quali in Internet. Di seguito vengono riportati alcuni dei tipi più comuni:

- ***Un virus*** è un codice dannoso che si copia e si diffonde in maniera automatica, spesso passando inosservato fino al compimento del danno. Alcuni virus rappresentano una minaccia seria, poiché eliminano o modificano direttamente i file, mentre altri agiscono in maniera apparentemente innocua, ad esempio durante la riproduzione di un brano musicale. Tuttavia, tutti i virus sono pericolosi a causa della capacità di base di moltiplicarsi. Anche un virus semplice è in grado di assorbire tutta la memoria di un computer in un istante causando danni.

- ***Il worm*** è una sottocategoria di virus che, a differenza dei virus normali, non necessita di un oggetto "trasportatore" a cui collegarsi; si invia automaticamente ad altri computer, solitamente tramite e-mail, provocando spesso sovraccarichi sui server e-mail e sui sistemi di rete.

- ***Spyware*** si definisce solitamente come una categoria di malware (*malware = qualsiasi software dannoso, virus compresi*) che comprende alcuni programmi, in genere trojan horse, il cui scopo è quello di appropriarsi di informazioni personali, password, numeri delle carte di credito o infiltrarsi in un computer consentendo all'autore dell'attacco di assumere il controllo in modalità remota, ovviamente senza che il proprietario del computer ne sia a conoscenza o abbia dato il proprio consenso.

- I ***programmi potenzialmente indesiderati*** sono un tipo di spyware che può essere o meno pericoloso per il computer. Un esempio specifico di PUP è l'adware, un software progettato per distribuire annunci, solitamente tramite la visualizzazione di popup. Può essere fastidioso ma non realmente dannoso.

- ***I cookie di rilevamento*** possono inoltre essere considerati come un tipo di spyware, in quanto si tratta di piccoli file archiviati nel browser Web e inviati automaticamente al sito Web principale quando lo si visita di nuovo, e possono contenere dati quali la cronologia di esplorazione e altre informazioni simili.

- ***Exploit*** è un codice dannoso che sfrutta un'imperfezione o una vulnerabilità di un sistema operativo, un browser Internet o un altro programma fondamentale.

- ***Il phishing*** è un tentativo di acquisire dati personali sensibili fingendosi un'organizzazione nota e affidabile. In genere, le vittime potenziali vengono contattate tramite messaggi e-mail inviati in blocco in cui vengono richiesti, ad esempio, i dati del conto bancario. A questo scopo, gli utenti vengono invitati a seguire il collegamento fornito che li indirizza a un sito Web della banca falso.

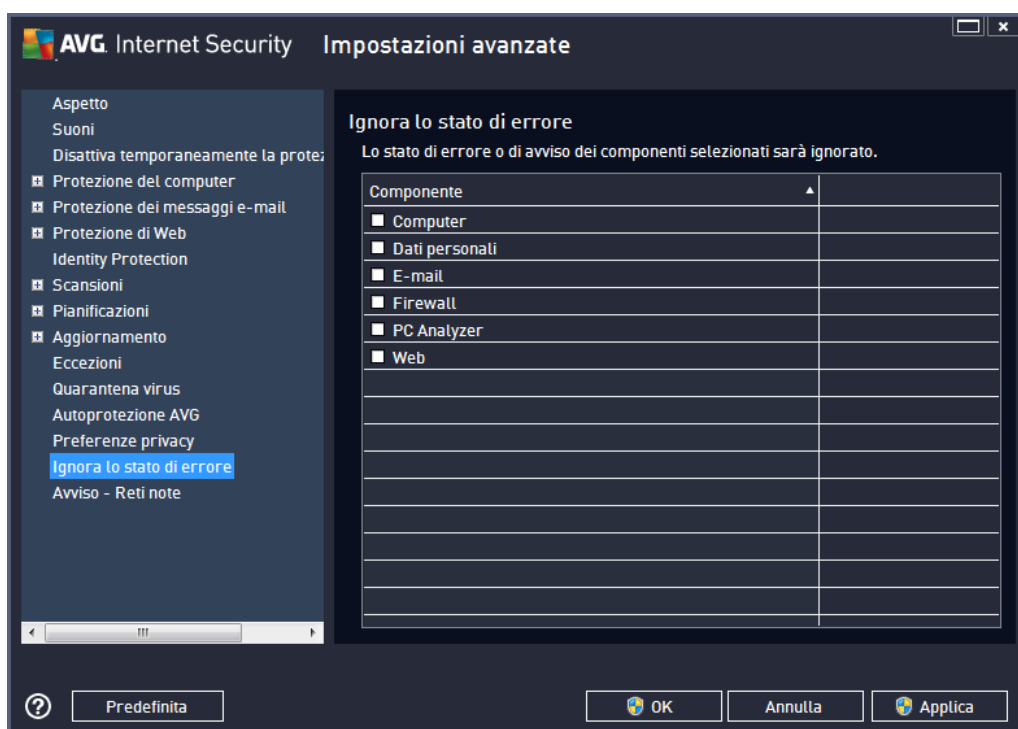
- ***Gli hoax*** sono messaggi e-mail inviati in blocco contenenti informazioni pericolose, allarmanti o semplicemente inutili e fastidiose. Molte delle minacce sopraelencate per diffondersi utilizzano i messaggi e-mail hoax.

- ***I siti Web dannosi*** sono quei siti che installano deliberatamente software dannoso nel computer, in modo simile ai siti manomessi, anche se questi ultimi sono siti Web legittimi

che sono stati compromessi da visitatori che hanno introdotto infezioni.

Per proteggere il PC da tutti questi tipi di minaccia, AVG Internet Security 2013 include componenti dedicati. Per una breve descrizione, consultare il capitolo Panoramica dei componenti.

9.15. Ignora lo stato di errore

Nella finestra di dialogo ***Ignora lo stato di errore*** è possibile selezionare i componenti in merito ai quali non si desidera ricevere informazioni:

Per impostazione predefinita, in questo elenco non è selezionato alcun componente. Ciò significa che se per un qualsiasi componente si verifica uno stato di errore, se ne verrà immediatamente informati tramite:

- l'icona presente nella barra delle applicazioni: quando tutte le parti di AVG funzionano correttamente, l'icona viene visualizzata in quattro colori; se si verifica un errore, l'icona viene visualizzata con un punto esclamativo giallo,

- una descrizione del problema esistente visualizzata nella sezione Informazioni sullo stato di protezione della finestra principale di AVG

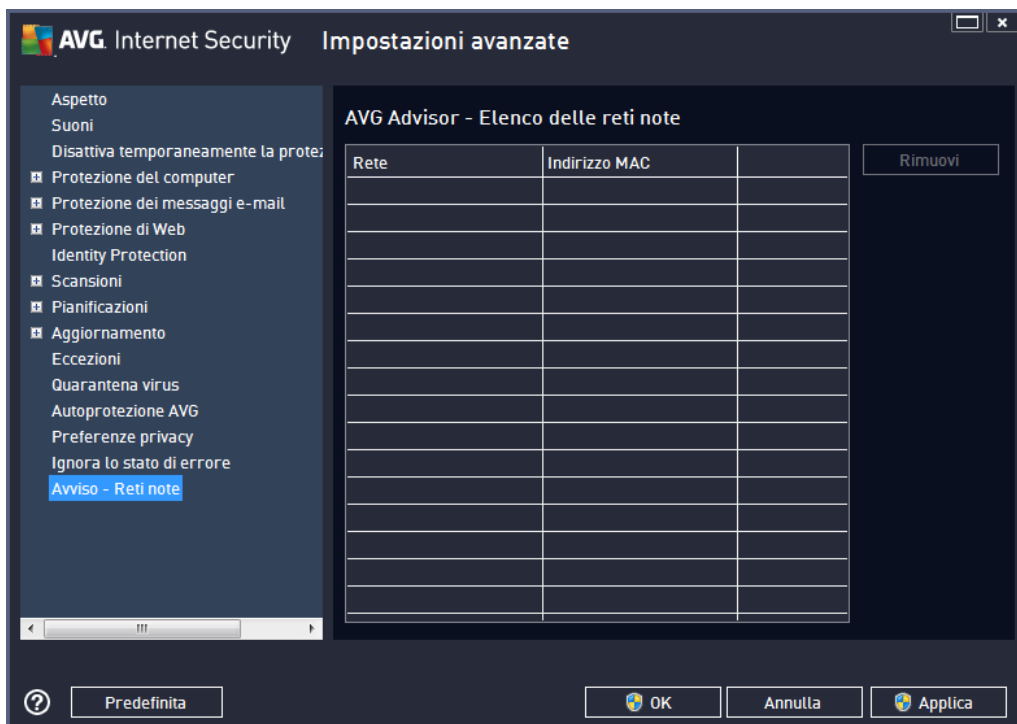
Potrebbe verificarsi una situazione in cui, per qualsiasi motivo, risulti necessario disattivare un componente temporaneamente. ***Questa operazione tuttavia non è consigliabile, si dovrebbe tentare di mantenere attivati tutti i componenti in modo permanente e con la configurazione predefinita***. Ma nel caso si verifichi questa situazione, l'icona presente nella barra delle applicazioni segnala automaticamente lo stato di errore del componente. In casi del genere, tuttavia, non è possibile parlare di errore effettivo, poiché la condizione è stata indotta deliberatamente dall'utente e si è consapevoli del potenziale rischio. Nel contempo, una volta che viene visualizzata in grigio,

l'icona non può più segnalare eventuali errori ulteriori che potrebbero verificarsi.

Per gestire situazioni simili, all'interno della finestra di dialogo ***Ignora lo stato di errore*** è possibile selezionare i componenti che potrebbero trovarsi in stato di errore (*o disattivati*) in merito ai quali non si desidera ricevere informazioni. Selezionare il pulsante ***OK***per confermare.

9.16. Avviso – Reti note

In AVG Advisor è inclusa una funzionalità che monitora le reti a cui si esegue la connessione e, se viene rilevata una nuova rete *(con un nome di rete già utilizzato, che potrebbe generare confusione)*, visualizza una notifica e suggerisce di verificare la sicurezza della rete. Se si considera sicura la nuova rete, è possibile salvarla in questo elenco *(tramite il collegamento fornito nella notifica di AVG Advisor che scorre sulla barra delle applicazioni quando viene rilevata una rete sconosciuta. Per ulteriori dettagli vedere il capitolo su AVG Advisor)*. AVG Advisor memorizzerà gli attributi univoci della rete *(in particolare l'indirizzo MAC)* e in seguito non visualizzerà la notifica. Ogni rete a cui si esegue la connessione verrà automaticamente considerata come rete conosciuta e aggiunta all'elenco. È possibile eliminare singole voci facendo clic sul pulsante ***Rimuovi***: la rete corrispondente verrà nuovamente considerata sconosciuta e potenzialmente non sicura.

In questa finestra di dialogo è possibile controllare quali reti sono considerate conosciute:

Nota: *la funzione reti conosciute in AVG Advisor non è supportata in Windows XP a 64 bit.*

10. Impostazioni Firewall

La finestra di dialogo di configurazione del Firewall viene aperta in una nuova finestra in cui è possibile impostare parametri avanzati del componente in varie finestre di dialogo. La finestra di dialogo di configurazione viene aperta in una nuova finestra in cui è possibile modificare parametri avanzati del componente in varie finestre di dialogo. È possibile visualizzare la configurazione in modalità di base o avanzata. Quando l'utente visualizza la finestra di dialogo di configurazione per la prima volta, questa viene aperta nella versione di base e consente la modifica dei seguenti parametri:

- Generale
- Applicazioni
- Condivisione file e stampanti

Nella parte inferiore della finestra di dialogo è presente il pulsante ***Modalità avanzata***. Far clic sul pulsante per visualizzare ulteriori elementi nell'esplorazione della finestra di dialogo per la configurazione molto avanzata del componente Firewall:

- Impostazioni avanzate
- Reti definite
- Servizi di Sistema
- Log

Tuttavia, il produttore del software ha impostato tutti i componenti di AVG Internet Security 2013 per fornire prestazioni ottimali. A meno che non sussista un motivo valido, si consiglia di non modificare la configurazione predefinita. Le eventuali modifiche alle impostazioni devono essere eseguite solo da utenti esperti!

10.1. Generale

La finestra di dialogo ***Informazioni generali*** fornisce una panoramica di tutte le modalità Firewall disponibili. La selezione corrente della modalità Firewall può essere modificata semplicemente selezionando un'altra modalità dal menu.

Tuttavia, il produttore del software ha impostato tutti i componenti di AVG Internet Security 2013 per fornire prestazioni ottimali. A meno che non sussista un motivo valido, si consiglia di non modificare la configurazione predefinita. Le eventuali modifiche alle impostazioni devono essere eseguite solo da utenti esperti!

Il componente Firewall consente di definire le regole di protezione specifiche a seconda che si tratti di un computer presente in un dominio, di un computer autonomo o perfino di un notebook. Ogni opzione richiede un livello diverso di protezione e i livelli sono coperti dalle rispettive modalità. In breve, una modalità Firewall è una specifica configurazione del componente Firewall ed è possibile utilizzare diverse di queste configurazioni predefinite:

- ***Automatica***: in questa modalità il componente Firewall gestisce tutto il traffico di rete automaticamente. Non verrà richiesto l'intervento dell'utente. Il componente Firewall consentirà la connessione a tutte le applicazioni note e contemporaneamente verrà creata una regola che indica che tale applicazione può connettersi sempre in futuro. Per altre applicazioni, Firewall deciderà se consentire o bloccare la connessione in base al comportamento dell'applicazione. Tuttavia, in questa situazione non verrà creata alcuna regola e l'applicazione verrà controllata nuovamente quando tenta di connettersi. ***La modalità automatica è abbastanza discreta ed è consigliata per la maggior parte degli utenti.***

- ***Interattiva***: questa modalità è utile se si desidera controllare completamente tutto il traffico di rete in ingresso e in uscita dal computer. Il componente Firewall monitorerà il traffico e notificherà all'utente ogni tentativo di comunicazione o trasferimento dati, permettendo all'utente di consentire o bloccare i tentativi come desidera. Opzione consigliata solo per utenti esperti.

- ***Blocca l'accesso a Internet***: la connessione a Internet viene bloccata completamente, è impossibile accedere a Internet e nessuno può accedere al computer dall'esterno. Solo per uso eccezionale e per breve tempo.

- ***Disattiva la protezione Firewall***: la disattivazione del Firewall consentirà tutto il traffico di rete in entrata e in uscita dal computer. Di conseguenza, il computer sarà esposto agli attacchi di hacker. Valutare sempre questa opzione con attenzione.

Tenere presente che una modalità automatica specifica è disponibile anche nel Firewall. Questa

modalità viene attivata in modo invisibile se i componenti Protezione del computer o Identity Protection vengono disattivati rendendo il computer più vulnerabile. In tali casi, il componente Firewall consentirà automaticamente solo le applicazioni note e assolutamente sicure. Per tutti gli altri casi, verrà richiesto all'utente come procedere. Ciò consente di ovviare alla disattivazione dei componenti di protezione e di mantenere il computer protetto.

10.2. Applicazioni

Nella finestra di dialogo ***Applicazioni*** sono elencate tutte le applicazioni che hanno tentato di comunicare in rete fino ad ora e le icone per l'azione assegnata:

Le applicazioni visualizzate in ***Elenco di applicazioni*** sono state rilevate sul computer (*e dispongono delle rispettive azioni assegnate*). È possibile utilizzare i seguenti tipi di azione:

- : consenti comunicazione per tutte le reti
- : blocca comunicazione
- : visualizza finestra di dialogo di conferma (*l'utente potrà decidere se consentire o bloccare la comunicazione quando l'applicazione tenterà di comunicare in rete*)
- : impostazioni avanzate definite

Tenere presente che è possibile rilevare solo le applicazioni già installate. Per impostazione predefinita, quando la nuova applicazione tenta di connettersi in rete per la prima volta, il componente Firewall crea automaticamente una regola in base al Database attendibile oppure chiede all'utente se consentire o bloccare la comunicazione. Nel secondo caso, sarà possibile salvare la risposta come regola permanente (che verrà quindi elencata in questa finestra di dialogo).

Naturalmente, è anche possibile definire immediatamente le regole per la nuova applicazione. In

questa finestra di dialogo fare clic su ***Aggiungi*** e immettere i dettagli dell'applicazione.

Oltre alle applicazioni, nell'elenco sono incluse anche due voci speciali. ***Regole per applicazione prioritaria*** (*nella parte superiore dell'elenco*). Queste regole sono preferenziali e vengono sempre applicate prima delle regole di ogni singola applicazione. ***Regole per altre applicazioni*** (*nella parte inferiore dell'elenco*). Queste regole sono utilizzate come "ultima istanza" quando non si applicano regole di applicazioni specifiche, ad esempio per un'applicazione sconosciuta e non definita. Selezionare l'azione che deve essere attivata se tale applicazione effettuasse un tentativo di comunicazione in rete: Blocca *(la comunicazione sarà sempre bloccata)*, Consenti *(la comunicazione sarà consentita su tutte le reti)*, Richiedi *(l'utente dovrà specificare se la comunicazione deve essere consentita o bloccata)*. ***Questi elementi presentano opzioni di impostazione diverse dalle applicazioni comuni e sono destinati esclusivamente agli utenti esperti. Si consiglia di non modificare le impostazioni.***

Pulsanti di controllo

Per modificare l'elenco, utilizzare i seguenti pulsanti di controllo:

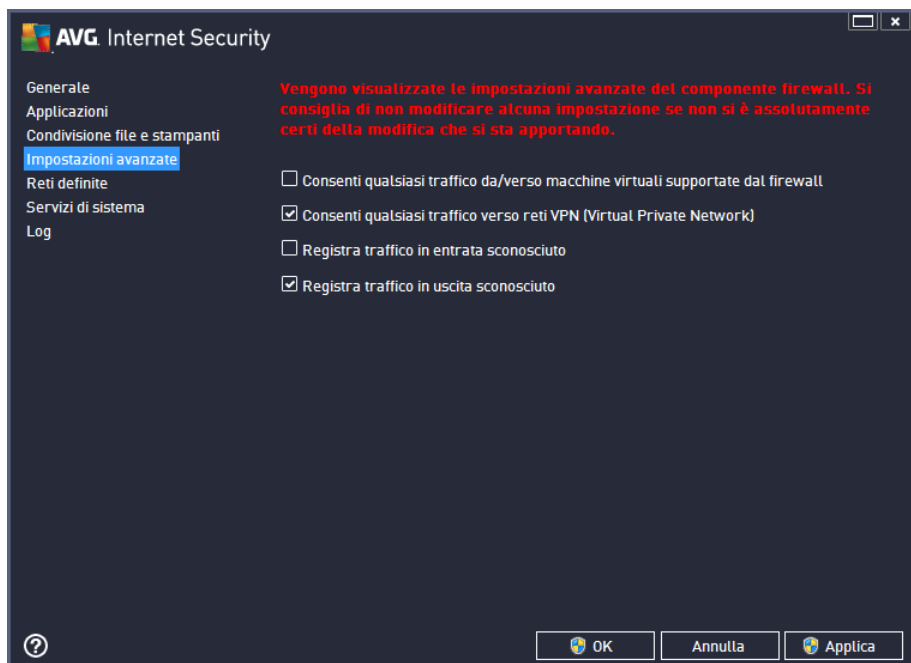
- ***Aggiungi***: consente di aprire una finestra di dialogo vuota per la definizione di nuove regole delle applicazioni.
- ***Modifica***: consente di aprire la stessa finestra di dialogo completa di dati per la modifica di un insieme di regole per un'applicazione esistente.
- ***Elimina***: consente di rimuovere dall'elenco l'applicazione selezionata.

10.3. Condivisione file e stampanti

Condivisione di file e stampanti significa condividere qualsiasi file o cartella contrassegnato come "Condiviso" in Windows, in unità disco comuni, stampanti, scanner e dispositivi simili. È preferibile condividere tali elementi solo all'interno di reti considerate sicure *(ad esempio a casa, in ufficio o a scuola)*. Tuttavia, se si è connessi a una rete pubblica *(ad esempio, al Wi-Fi dell'aeroporto o di un Internet Point)*, è consigliabile non condividere nulla. AVG Firewall può bloccare o consentire facilmente la condivisione e permettere all'utente di salvare la scelta eseguita per le reti già visitate.

Nella finestra di dialogo ***Condivisione file e stampanti*** è possibile modificare la configurazione della condivisione file e stampanti e le reti attualmente connesse. Con Windows XP, il nome della rete corrisponde alla denominazione scelta per la rete specifica durante la prima connessione. Con Windows Vista e versioni successive, il nome della rete viene ricavato automaticamente dal Centro connessioni di rete e condivisione.

10.4. Impostazioni avanzate

Le modifiche nella finestra di dialogo Impostazioni avanzate sono riservate ESCLUSIVAMENTE agli UTENTI ESPERTI.

La finestra di dialogo ***Impostazioni avanzate*** consente di attivare/disattivare i seguenti parametri del componente Firewall:

- ***Consenti qualsiasi traffico da/verso macchine virtuali supportate dal Firewall***: supporto per la connessione di rete in macchine virtuali come VMWare.
- ***Consenti qualsiasi traffico verso reti VPN (Virtual Private Network)***: supporto per connessioni VPN *(utilizzato per connettersi a computer remoti)*.
- ***Registra traffico sconosciuto in entrata/in uscita***: tutti i tentativi di comunicazione *(entranti/uscenti)* da parte di applicazioni sconosciute verranno registrati nel Log Firewall.

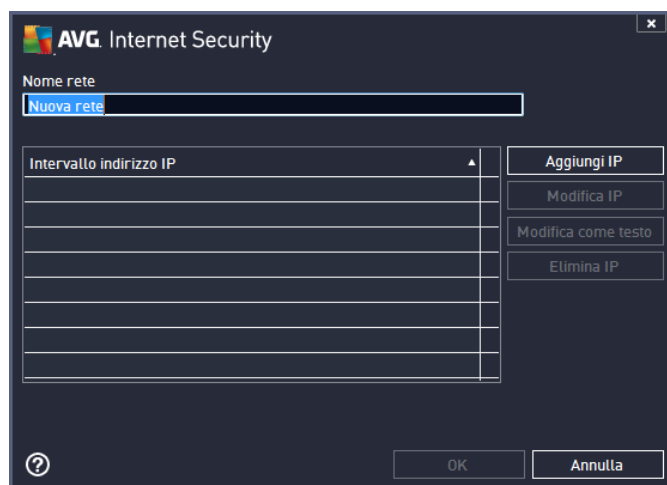
10.5. Reti definite

Le eventuali modifiche alla finestra di dialogo Reti definite sono riservate ESCLUSIVAMENTE agli UTENTI ESPERTI.

Nella finestra di dialogo ***Reti definite*** è disponibile un elenco di tutte le reti a cui è connesso il computer. L'elenco fornisce le seguenti informazioni su ciascuna rete rilevata:

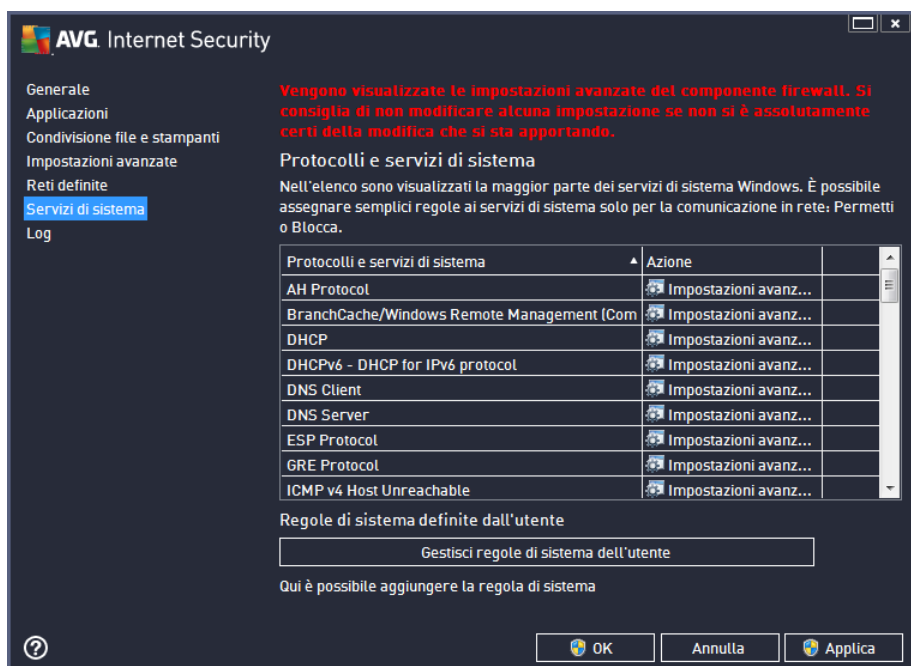
- ***Reti***: fornisce l'elenco dei nomi di tutte le reti a cui è connesso il computer.
- ***Intervallo indirizzi IP***: ogni rete verrà rilevata automaticamente e specificata sotto forma di intervallo di indirizzi IP.

Pulsanti di controllo

- ***Aggiungi rete***: consente di aprire una nuova finestra di dialogo in cui è possibile modificare i parametri della rete appena definita, ovvero specificare il ***Nome rete***e l'***intervallo indirizzi IP***:

- ***Modifica rete***: consente di aprire la finestra di dialogo ***Proprietà rete*** (*vedere sopra*) dove è possibile modificare i parametri di una rete già definita (*questa finestra di dialogo è identica alla finestra di dialogo per l'aggiunta di nuove reti, vedere la descrizione nel paragrafo precedente*).

- ***Elimina rete***: consente di rimuovere il riferimento a una rete selezionata dall'elenco delle reti.

10.6. Servizi di sistema

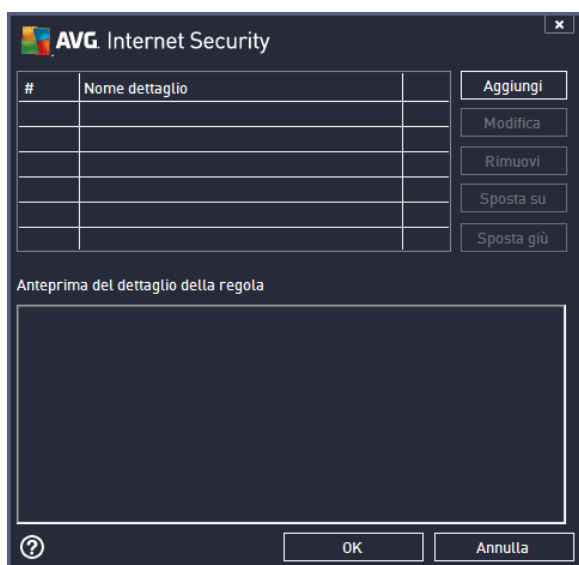
Le modifiche alla finestra di dialogo Protocolli e servizi di sistema sono riservate ESCLUSIVAMENTE agli UTENTI ESPERTI.

La finestra di dialogo ***Protocolli e servizi di sistema*** elenca i protocolli e i servizi di sistema standard di Windows che potrebbero dover comunicare sulla rete. Il grafico presenta le seguenti

colonne:

- ***Protocolli e servizi di sistema***: questa colonna mostra il nome del rispettivo servizio di sistema.
- ***Azione***: questa colonna mostra un'icona per l'azione assegnata:
  - o Consenti comunicazione per tutte le reti
  - o Blocca comunicazione

Per modificare le impostazioni delle voci dell'elenco (*incluse le azioni assegnate*), fare clic con il pulsante destro del mouse sulla voce desiderata e selezionare ***Modifica***. ***Tuttavia, la modifica delle regole di sistema dovrebbe essere eseguita solo da utenti avanzati. È consigliabile non modificare le regole di sistema.***

Regole di sistema definite dall'utente

Per aprire una nuova finestra di dialogo per la definizione di una regola dei servizi di sistema personalizzata (*vedere la seguente immagine*), selezionare il pulsante ***Gestisci regole di sistema dell'utente***. La stessa finestra di dialogo verrà visualizzata se si decide di modificare la configurazione di qualsiasi elemento presente nell'elenco dei protocolli e dei servizi di sistema. La sezione superiore di questa finestra di dialogo mostra una panoramica di tutti i dettagli della regola di sistema modificata, la sezione inferiore mostra quindi il dettaglio selezionato. I dettagli delle regole possono essere modificati, aggiunti o eliminati tramite gli appositi pulsanti:

Tenere presente che queste impostazioni delle regole dettagliate sono avanzate e destinate innanzitutto agli amministratori di rete che necessitano del controllo completo della configurazione del componente Firewall. Se non si conoscono i tipi di protocollo di comunicazione, i numeri delle porte di rete, le definizioni degli indirizzi IP e così via, non modificare queste impostazioni. Se fosse necessario modificare la configurazione, consultare i file della Guida della rispettiva finestra di dialogo per dettagli specifici.

10.7. Log

Le eventuali modifiche alla finestra di dialogo Log sono riservate ESCLUSIVAMENTE agli UTENTI ESPERTI.

La finestra di dialogo ***Log*** consente di visualizzare l'elenco di tutte le azioni e gli eventi registrati di Firewall con una descrizione dettagliata dei parametri rilevanti mostrata in due schede:

- ***Log traffico***: questa scheda fornisce informazioni sull'attività di tutte le applicazioni che hanno tentato di connettersi alla rete. Per ognuna di queste, saranno incluse informazioni relative a ora dell'evento, nome dell'applicazione, rispettiva azione log, nome utente, PID, direzione del traffico, tipo di protocollo, numeri delle porte remote e locali e informazioni sull'indirizzo IP remoto e locale.

- ***Log database attendibile***: il *Database attendibile* è un database interno di AVG che raccoglie informazioni sulle applicazioni certificate e attendibili che saranno sempre autorizzate a comunicare in linea. La prima volta in cui una nuova applicazione tenta di connettersi alla rete (*ossia quando non è ancora stata specificata alcuna regola firewall per tale applicazione*), è necessario stabilire se la comunicazione di rete deve essere consentita per tale applicazione. Innanzitutto, AVG effettua una ricerca nel *Database attendibile*. Se l'applicazione è elencata, sarà automaticamente autorizzata ad accedere alla rete. Se nel database non sono presenti informazioni sull'applicazione, verrà richiesto in una nuova finestra di dialogo se si desidera autorizzare l'applicazione ad accedere alla rete.

Pulsanti di controllo

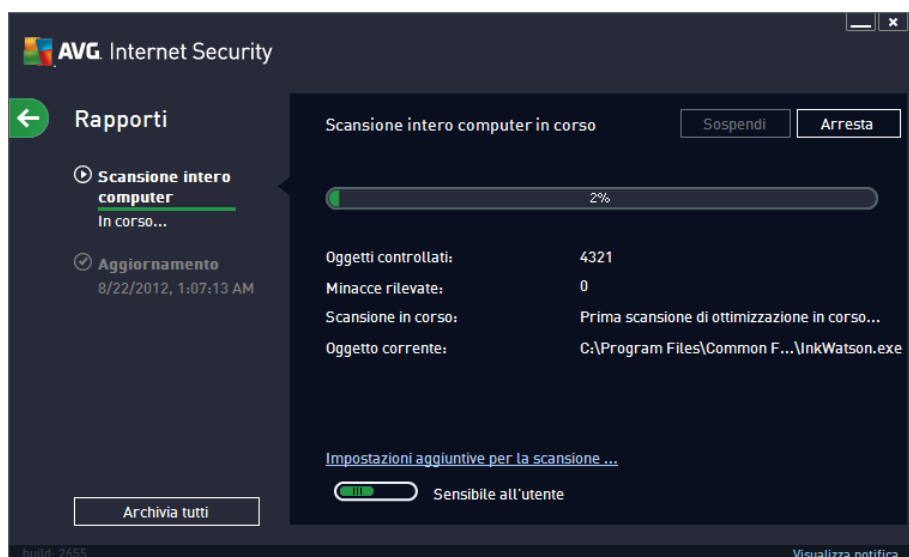
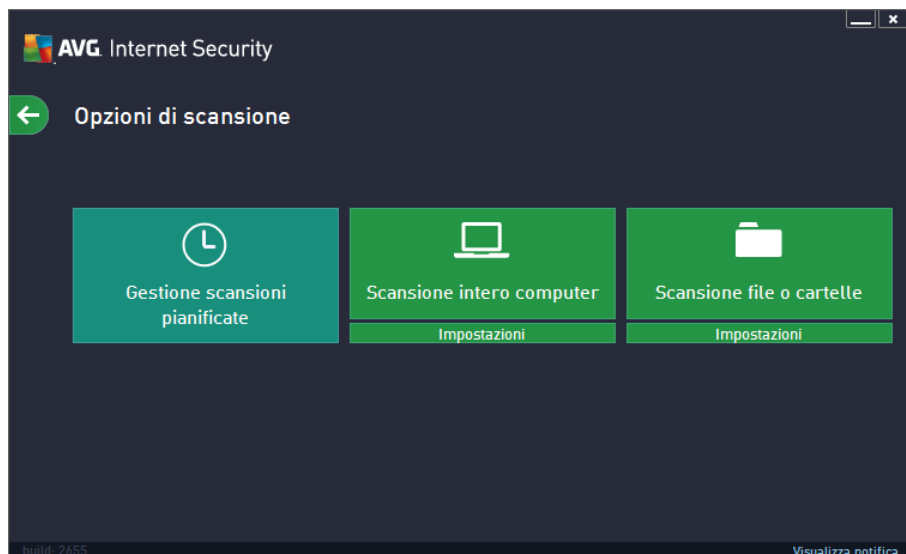
- ***Aggiorna elenco***: tutti i parametri registrati possono essere ordinati in base all'attributo selezionato: cronologicamente (*date*) o alfabeticamente (*altre colonne*). È sufficiente fare clic sull'intestazione di colonna pertinente. Utilizzare il pulsante ***Aggiorna elenco*** per aggiornare le informazioni visualizzate.

- ***Elimina log***: fare clic per eliminare tutte le voci presenti nel grafico.

11. Scansione AVG

Per impostazione predefinita, **AVG Internet Security 2013** non esegue alcuna scansione, poiché dopo la scansione iniziale *(che all'utente viene richiesto di avviare*), il computer dovrebbe essere perfettamente protetto dai componenti permanenti di **AVG Internet Security 2013** che sono sempre attivi e non lasciano entrare codice dannoso nel sistema. Naturalmente, è possibile pianificare l'esecuzione di una scansione a intervalli regolari o avviare manualmente una scansione in qualsiasi momento in base alle esigenze.

L'interfaccia di scansione di AVG è accessibile dall'interfaccia utente principale tramite il pulsante suddiviso graficamente in due sezioni: Esegui scansione

- ***Esegui scansione***: selezionare il pulsante per il collegamento per avviare subito la Scansione intero computer e visualizzare l'avanzamento e i risultati relativi nella finestra Rapporti aperta automaticamente:

- ***Opzioni***: selezionare questo pulsante *(visualizzato graficamente come tre linee orizzontali in un campo verde)* per aprire la finestra di dialogo ***Opzioni di scansione*** in cui è possibile gestire le scansioni pianificate e modificare i parametri diScansione intero computer / Scansione file o cartelle:

Nella finestra di dialogo ***Opzioni di scansione*** è possibile visualizzare tre sezioni principali di configurazione della scansione:

- ***Gestione scansioni pianificate***: fare clic su questa opzione per aprire una nuova finestra di dialogo con una panoramica di tutte le scansioni pianificate. Prima di definire delle scansioni personalizzate, nell'elenco sarà possibile visualizzare solo una scansione pianificata predefinita dal fornitore del software. Per impostazione predefinita, la scansione è disattivata. Per attivarla, fare clic con il pulsante destro del mouse sulla scansione e selezionare l'opzione *Abilita attività* dal menu di scelta rapida. Dopo aver abilitato la scansione pianificata, è possibile modificare la relativa configurazione tramite il pulsante *Modifica pianificazione scansione*. Inoltre, è possibile fare clic sul pulsante *Aggiungi scansione pianificata* per creare una nuova pianificazione di scansione personalizzata.

- ***Scansione intero computer / Impostazioni*** : il pulsante è suddiviso in due sezioni. Fare clic sull'opzione *Scansione intero computer* per avviare immediatamente la scansione dell'intero computer *(per dettagli sulla scansione dell'intero computer vedere il relativo capitolo Scansioni predefinite / Scansione intero computer)*. Facendo clic sulla sezione *Impostazioni* sottostante è possibile accedere alla finestra di dialogo di configurazione della scansione intero computer.

- ***Scansione file o cartelle / Impostazioni*** : anche questo pulsante è suddiviso in due sezioni. Fare clic sull'opzione *Scansione file o cartelle* per avviare immediatamente la scansione delle aree selezionate del computer*(per dettagli sulla scansione dei file e delle cartelle selezionati, vedere il relativo capitolo Scansioni predefinite / Scansione file o cartelle)*. Facendo clic sulla sezione *Impostazioni* sottostante è possibile accedere alla finestra di dialogo di configurazione della scansione file o cartelle.

11.1. Scansioni predefinite

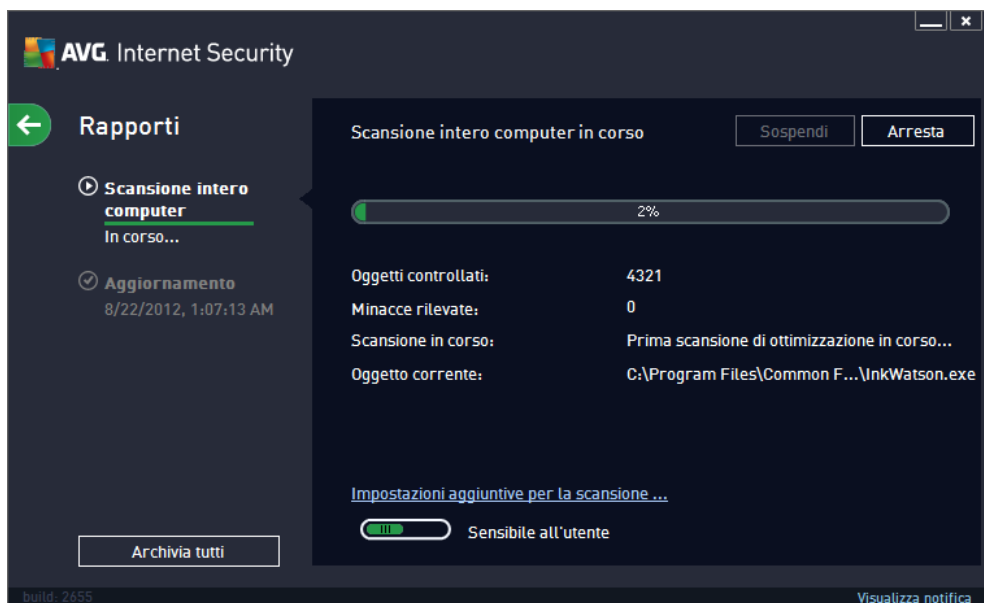
Una delle funzioni principali di **AVG Internet Security 2013** è la scansione su richiesta. I controlli su richiesta sono progettati per eseguire la scansione di varie parti del computer quando si sospetta una possibile infezione da virus. Comunque, si consiglia di eseguire regolarmente tali verifiche anche se non si ritiene che siano presenti virus nel computer.

In **AVG Internet Security 2013** sono disponibili i seguenti tipi di scansione predefiniti dal fornitore del software:

11.1.1. Scansione intero computer

Scansione intero computer consente di eseguire scansioni dell'intero computer per il rilevamento di possibili infezioni e/o di programmi potenzialmente indesiderati. Questo controllo eseguirà la scansione di tutti i dischi rigidi nel computer, rileverà e correggerà i virus trovati oppure sposterà l'infezione rilevata in Quarantena virus. È necessario pianificare la scansione dell'intero computer almeno una volta la settimana.

Avvio della scansione

La ***Scansione intero computer*** può essere avviata direttamente dall'interfaccia utente principale facendo clic sul pulsante***Esegui scansione***. Non è necessario configurare ulteriori impostazioni specifiche per questo tipo di scansione. La scansione verrà avviata immediatamente. Nella finestra di dialogo ***Scansione intero computer*** (*vedere la schermata*) è possibile visualizzare l'avanzamento della scansione e i relativi risultati. La scansione può essere temporaneamente interrotta (***Sospendi***) oppure annullata (***Arresta***) se necessario.

Modifica della configurazione della scansione

È possibile modificare la configurazione della ***Scansione intero computer*** nella finestra di dialogo ***Scansione intero computer – Impostazioni*** *(tale finestra è accessibile tramite il collegamento Impostazioni per Scansione intero computer nella finestra Opzioni di scansione).* ***Si consiglia di mantenere le impostazioni predefinite e di modificarle solo se esiste un reale motivo per farlo.***

Nell'elenco dei parametri di scansione è possibile attivare/disattivare parametri specifici in base alle esigenze:

- ***Correggi/Rimuovi infezioni da virus senza richiedere conferma*** *(attivata per impostazione predefinita)*: se viene identificato un virus durante la scansione, può essere corretto automaticamente se è disponibile una soluzione. Se il file infetto non può essere corretto automaticamente, l'oggetto infetto verrà spostato in Quarantena virus.

- ***Segnala programmi potenzialmente indesiderati e minacce spyware*** *(attivata per impostazione predefinita)*: selezionare questa casella di controllo per attivare la scansione per ricercare spyware e virus. Gli spyware rappresentano una categoria di malware anomala: anche se solitamente costituiscono un rischio per la sicurezza, alcuni di questi programmi possono essere installati intenzionalmente. Si consiglia di mantenere questa funzionalità attivata in quanto consente di aumentare la protezione del computer.

- ***Segnala set potenziati di programmi potenzialmente indesiderati*** *(disattivata per impostazione predefinita)*: selezionare questa casella di controllo per rilevare pacchetti estesi di spyware, ovvero programmi perfettamente normali e innocui al momento dell'acquisto diretto presso il produttore, ma utilizzabili a scopi dannosi successivamente. Si tratta di una precauzione aggiuntiva che aumenta ulteriormente la protezione del computer, ma che potrebbe bloccare programmi legittimi, pertanto l'opzione è disattivata per impostazione predefinita.

- ***Scansione dei cookie di rilevamento*** *(disattivata per impostazione predefinita)*: questo parametro specifica che i cookie devono essere rilevati *(i cookie HTTP vengono utilizzati per autenticare, rilevare e mantenere informazioni specifiche sugli utenti, quali le preferenze dei siti o il contenuto dei carrelli elettronici)*.

- ***Scansione all'interno degli archivi*** *(disattivata per impostazione predefinita)*: questo parametro specifica che la scansione deve controllare tutti i file inclusi all'interno di un archivio, quali ZIP, RAR e così via.

- ***Usa analisi euristiche*** *(attivata per impostazione predefinita)*: l'analisi euristica *(emulazione*

dinamica delle istruzioni dell'oggetto sottoposto a scansione in un ambiente informatico virtuale) sarà uno dei metodi utilizzati per il rilevamento di virus durante la scansione.

- ***Scansione ambiente di sistema*** *(attivata per impostazione predefinita)*: la scansione verrà eseguita anche sulle aree di sistema del computer.

- ***Attiva scansione completa*** *(disattivata per impostazione predefinita)*: in situazioni specifiche *(ad esempio se si sospetta che il computer sia stato infettato)* per maggiore sicurezza è possibile selezionare questa opzione per attivare gli algoritmi di scansione più completi che esamineranno anche le aree del computer che difficilmente vengono infettate. Tenere presente tuttavia che questo metodo è piuttosto dispendioso in termini di tempo.

- ***Impostazioni di scansione aggiuntive***: il collegamento consente di aprire una nuova finestra di dialogo Impostazioni di scansione aggiuntive in cui è possibile specificare i seguenti parametri:

  - ***Opzioni arresto computer***: consente di decidere se il computer deve essere arrestato automaticamente al termine del processo di scansione. Dopo aver confermato questa opzione (***Arresta computer al completamento della scansione***), viene attivata una nuova opzione che consente l'arresto del computer anche se è correntemente bloccato (***Forza arresto se il computer è bloccato***).

  - ***Tipi di file per la scansione***: specificare se si desidera sottoporre a scansione:

    - ***Tutti i tipi di file*** con l'opzione per definire le eccezioni fornendo un elenco di estensioni di file separate da virgola da non sottoporre a scansione;

    - ***Tipi di file selezionati***: è possibile specificare che si desidera sottoporre a scansione solo file potenzialmente infettabili (*i file che non possono essere infettati non verranno sottoposti a scansione, ad esempio alcuni file di testo normale o altri file non eseguibili*), inclusi i file multimediali (*file video e audio, se*

non si seleziona questa casella, il tempo di scansione risulterà ulteriormente ridotto, poiché questi file sono spesso di grandi dimensioni e non facilmente infettabili dai virus.). Anche in questo caso, è possibile specificare tramite le estensioni quali file devono essere sempre sottoposti a scansione.

- Facoltativamente, è possibile effettuare la ***scansione dei file senza estensioni***: questa opzione è attivata per impostazione predefinita e si consiglia di non modificarla a meno che non siano presenti motivi validi per farlo. I file senza estensione sono piuttosto sospetti e devono essere sempre sottoposti a scansione.

- ***Regola la velocità di completamento della scansione***: è possibile utilizzare il dispositivo di scorrimento per modificare la priorità del processo di scansione. Per impostazione predefinita, questa opzione è impostata sul livello *Sensibile all'utente* per l'utilizzo automatico delle risorse. In alternativa, è possibile eseguire il processo di scansione più lentamente in modo da ridurre al minimo il carico sulle risorse di sistema (*utile quando è necessario lavorare al computer ma la durata della scansione non influisce*) o più velocemente con utilizzo delle risorse di sistema più elevato (*ad esempio quando l'utente è temporaneamente lontano dal computer*).

- ***Imposta rapporti di scansione aggiuntivi***: il collegamento consente di aprire una nuova finestra di dialogo ***Rapporti di scansione*** in cui è possibile selezionare quali tipi di rilevamenti segnalare.

Avviso: *queste impostazioni di scansione sono identiche ai parametri di una nuova scansione definita, come descritto nel capitolo [Scansione AVG / Pianificazione di scansioni/ Scansione da eseguire](). Se si decide di modificare la configurazione predefinita di* ***Scansione intero computer****, è possibile salvare le nuove impostazioni come configurazione predefinita da utilizzare per tutte le altre scansioni dell'intero computer.*

11.1.2. Scansione file o cartelle

Scansione file o cartelle: consente di eseguire la scansione delle sole aree del computer selezionate per la scansione (*cartelle, dischi rigidi, dischi floppy, CD selezionati e così via*). L'avanzamento della scansione nel caso di rilevamento di virus e relativo trattamento è uguale a quello della scansione dell'intero computer: gli eventuali virus rilevati vengono corretti o spostati in [Quarantena virus](). La scansione di file o cartelle specifiche può essere utilizzata per impostare controlli personalizzati e la relativa pianificazione in base alle esigenze.

Avvio della scansione

È possibile avviare la ***Scansione file o cartelle*** direttamente dalla finestra di dialogo [Opzioni di scansione]() facendo clic sul pulsante **Scansione file o cartelle**. Viene aperta una nuova finestra di dialogo ***Selezionare file o cartelle specifiche per la scansione***. Nella struttura del computer selezionare le cartelle che si desidera sottoporre a scansione. Il percorso di ciascuna cartella selezionata verrà generato automaticamente e visualizzato nella casella di testo nella parte superiore della finestra di dialogo. È inoltre possibile sottoporre a scansione una specifica cartella escludendo tutte le relative sottocartelle, a questo scopo scrivere un segno meno "**-**" davanti al percorso generato automaticamente (*vedere la schermata*). Per escludere l'intera cartella dalla scansione, utilizzare il parametro "!". Infine, per avviare la scansione, selezionare il pulsante ***Avvia scansione***. Il processo di scansione è praticamente identico a quello di [Scansione intero computer]().

Modifica della configurazione della scansione

È possibile modificare la configurazione di ***Scansione file o cartelle*** nella finestra di dialogo ***Scansione file o cartelle – Impostazioni*** *(tale finestra è accessibile tramite il collegamento Impostazioni per Scansione file o cartelle nella finestra [Opzioni di scansione]()).* ***Si consiglia di mantenere le impostazioni predefinite e di modificarle solo se esiste un reale motivo per farlo.***

Nell'elenco dei parametri di scansione è possibile attivare/disattivare parametri specifici in base alle esigenze:

- ***Correggi/Rimuovi infezioni da virus senza richiedere conferma*** *(attivata per impostazione predefinita)*: se viene identificato un virus durante la scansione, può essere corretto automaticamente se è disponibile una soluzione. Se il file infetto non può essere corretto automaticamente, l'oggetto infetto verrà spostato in Quarantena virus.

- ***Segnala programmi potenzialmente indesiderati e minacce spyware****(attivata per impostazione predefinita)*: selezionare questa casella di controllo per attivare la scansione per ricercare spyware e virus. Gli spyware rappresentano una categoria di malware anomala: anche se solitamente costituiscono un rischio per la sicurezza, alcuni di questi programmi possono essere installati intenzionalmente. Si consiglia di mantenere questa funzionalità attivata in quanto consente di aumentare la protezione del computer.

- ***Segnala set potenziati di programmi potenzialmente indesiderati*** *(disattivata per impostazione predefinita)*: selezionare questa casella di controllo per rilevare pacchetti estesi di spyware, ovvero programmi perfettamente normali e innocui al momento dell'acquisto diretto presso il produttore, ma utilizzabili a scopi dannosi successivamente. Si tratta di una precauzione aggiuntiva che aumenta ulteriormente la protezione del computer, ma che potrebbe bloccare programmi legittimi, pertanto l'opzione è disattivata per impostazione predefinita.

- ***Scansione dei cookie di rilevamento*** *(disattivata per impostazione predefinita)*: questo parametro specifica che i cookie devono essere rilevati *(i cookie HTTP vengono utilizzati per autenticare, rilevare e mantenere informazioni specifiche sugli utenti, quali le preferenze dei siti o il contenuto dei carrelli elettronici)*.

- ***Scansione all'interno degli archivi*** *(attivata per impostazione predefinita)*: questo parametro specifica che la scansione deve controllare tutti i file inclusi all'interno di un archivio, quali ZIP, RAR e così via.

- ***Usa analisi euristiche*** *(attivata per impostazione predefinita)*: l'analisi euristica *(emulazione dinamica delle istruzioni dell'oggetto sottoposto a scansione in un ambiente informatico virtuale)* sarà uno dei metodi utilizzati per il rilevamento di virus durante la scansione.

- ***Scansione ambiente di sistema*** *(disattivata per impostazione predefinita)*: la scansione verrà eseguita anche sulle aree di sistema del computer.

- ***Attiva scansione completa*** *(disattivata per impostazione predefinita)*: in situazioni specifiche *(ad esempio se si sospetta che il computer sia stato infettato)* per maggiore sicurezza è possibile selezionare questa opzione per attivare gli algoritmi di scansione più completi che esamineranno anche le aree del computer che difficilmente vengono infettate. Tenere presente tuttavia che questo metodo è piuttosto dispendioso in termini di tempo.

- ***Impostazioni di scansione aggiuntive***: il collegamento consente di aprire una nuova finestra di dialogo ***Impostazioni di scansione aggiuntive*** in cui è possibile specificare i seguenti parametri:

  - ***Opzioni arresto computer***: consente di decidere se il computer deve essere arrestato automaticamente al termine del processo di scansione. Dopo aver confermato questa opzione (***Arresta computer al completamento della scansione***), viene attivata una nuova opzione che consente l'arresto del computer anche se è correntemente bloccato (***Forza arresto se il computer è bloccato***).

  - ***Tipi di file per la scansione***: specificare se si desidera sottoporre a scansione:

    - ***Tutti i tipi di file*** con l'opzione per definire le eccezioni fornendo un elenco di estensioni di file separate da virgola da non sottoporre a scansione;

    - ***Tipi di file selezionati***: è possibile specificare che si desidera sottoporre a scansione solo file potenzialmente infettabili (*i file che non possono essere infettati non verranno sottoposti a scansione, ad esempio alcuni file di testo normale o altri file non eseguibili*), inclusi i file multimediali (*file video e audio, se non si seleziona questa casella, il tempo di scansione risulterà ulteriormente ridotto, poiché questi file sono spesso di grandi dimensioni e non facilmente infettabili dai virus.*). Anche in questo caso, è possibile specificare tramite le

estensioni quali file devono essere sempre sottoposti a scansione.

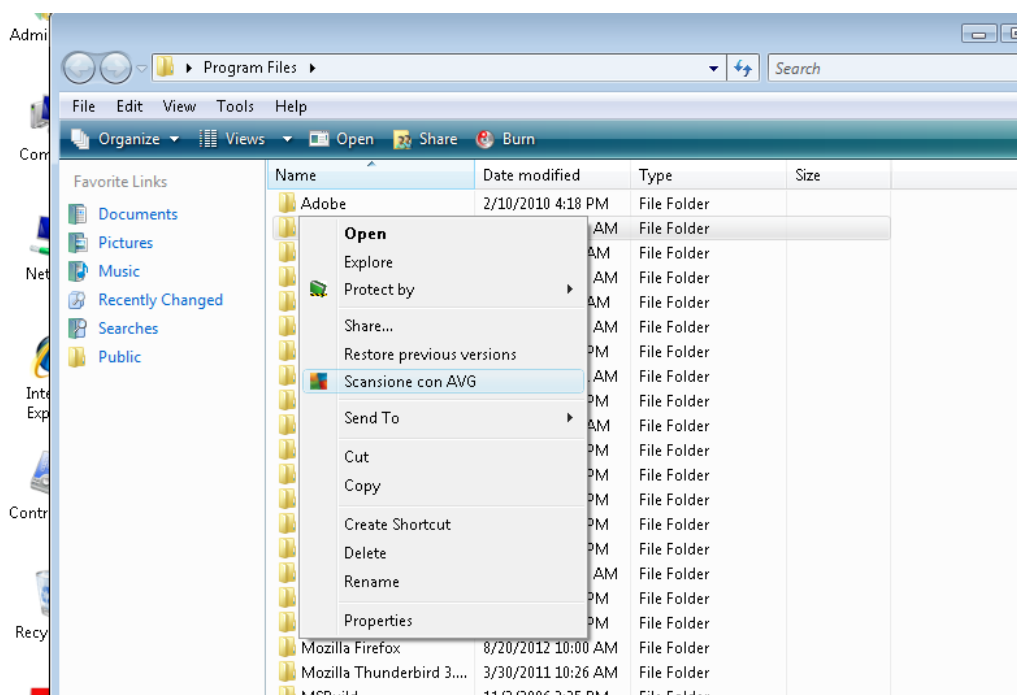
- Facoltativamente, è possibile effettuare la ***scansione dei file senza estensioni***: questa opzione è attivata per impostazione predefinita e si consiglia di non modificarla a meno che non siano presenti motivi validi per farlo. I file senza estensione sono piuttosto sospetti e devono essere sempre sottoposti a scansione.

- ***Regola la velocità di completamento della scansione***: è possibile utilizzare il dispositivo di scorrimento per modificare la priorità del processo di scansione. Per impostazione predefinita, questa opzione è impostata sul livello *Sensibile all'utente* per l'utilizzo automatico delle risorse. In alternativa, è possibile eseguire il processo di scansione più lentamente in modo da ridurre al minimo il carico sulle risorse di sistema (*utile quando è necessario lavorare al computer ma la durata della scansione non influisce*) o più velocemente con utilizzo delle risorse di sistema più elevato (*ad esempio quando l'utente è temporaneamente lontano dal computer*).

- ***Imposta rapporti di scansione aggiuntivi***: il collegamento consente di aprire una nuova finestra di dialogo ***Rapporti di scansione*** in cui è possibile selezionare quali tipi di rilevamenti segnalare:

Avviso: *queste impostazioni di scansione sono identiche ai parametri di una nuova scansione definita, come descritto nel capitolo* *Scansione AVG / Pianificazione di scansioni/ Scansione da eseguire*. *Se si decide di modificare la configurazione predefinita di* ***Scansione file o cartelle*** *è possibile salvare la nuova impostazione come configurazione predefinita da utilizzare per tutte le altre scansioni di file o cartelle specifiche. Inoltre, questa configurazione verrà utilizzata come modello per tutte le nuove scansioni pianificate (tutte le scansioni personalizzate si basano sulla configurazione corrente di Scansione file o cartelle).*

11.2. Scansione in Esplora risorse

Oltre alle scansioni predefinite avviate per l'intero computer o per le aree selezionate, **AVG Internet Security 2013** offre l'opzione di scansione rapida di un oggetto specifico direttamente nell'ambiente Esplora risorse. Se si desidera aprire un file sconosciuto e non si è sicuri del contenuto, è possibile decidere di eseguire un controllo su richiesta. Procedere come segue:

- In Esplora risorse evidenziare il file *o la cartella* che si desidera verificare
- Fare clic con il pulsante destro del mouse sull'oggetto per aprire il menu di scelta rapida
- Selezionare l'opzione ***Scansione con AVG*** per eseguire la scansione con **AVG Internet Security 2013**

11.3. Scansione da riga di comando

In **AVG Internet Security 2013** è possibile eseguire la scansione dalla riga di comando. Ad esempio, è possibile utilizzare questa opzione sui server oppure durante la creazione di uno script batch da avviare automaticamente dopo l'avvio del computer. Dalla riga di comando, è possibile avviare la scansione mentre nell'interfaccia utente grafica di AVG viene fornita la maggior parte dei parametri.

Per avviare la scansione di AVG dalla riga di comando, eseguire il seguente comando dalla cartella in cui è stato installato AVG:

- ***avgscanx*** per sistemi operativi a 32 bit
- ***avgscana*** per sistemi operativi a 64 bit

Sintassi del comando

La sintassi del comando è la seguente:

- ***avgscanx /parametro*** ... ad esempio ***avgscanx /comp*** per la scansione dell'intero computer

- ***avgscanx /parametro /parametro*** .. nel caso di più parametri, questi dovrebbero essere allineati in una riga e separati da uno spazio e dal carattere della barra (/)

- se per un parametro è necessario fornire un valore specifico (ad esempio, il parametro ***/ scan*** richiede informazioni relative alle aree del computer di cui eseguire la scansione ed è necessario fornire il percorso esatto della sezione selezionata), i valori vengono separati da punto e virgola. Ad esempio: ***avgscanx /scan=C:\;D:***

Parametri di scansione

Per visualizzare una panoramica completa dei parametri disponibili, digitare il rispettivo comando insieme al parametro /? o /HELP (ad esempio ***avgscanx /?***). Nota: l'unico parametro obbligatorio è / SCAN, che consente di specificare quali aree del computer devono essere sottoposte a scansione. Per spiegazioni più dettagliate delle opzioni, vedere la panoramica dei parametri da riga di comando.

Per eseguire la scansione, premere ***Invio***. Durante la scansione è possibile arrestare il processo premendo ***Ctrl+C*** oppure ***Ctrl+Pausa***.

Scansione CMD avviata dall'interfaccia grafica

Quando viene eseguita la modalità provvisoria di Windows, è inoltre possibile avviare la scansione da riga di comando dall'interfaccia utente grafica. La scansione verrà avviata dalla riga di comando. La finestra di dialogo ***Compositore riga di comando*** consente solo di specificare la maggior parte dei parametri di scansione nella comoda interfaccia grafica.

Poiché questa finestra di dialogo è accessibile solo nella modalità provvisoria di Windows, per ulteriori informazioni consultare il file della Guida aperto direttamente dalla finestra di dialogo.

11.3.1. Parametri scansione CMD

Di seguito viene fornito un elenco di tutti i parametri disponibili per la scansione della riga di comando:

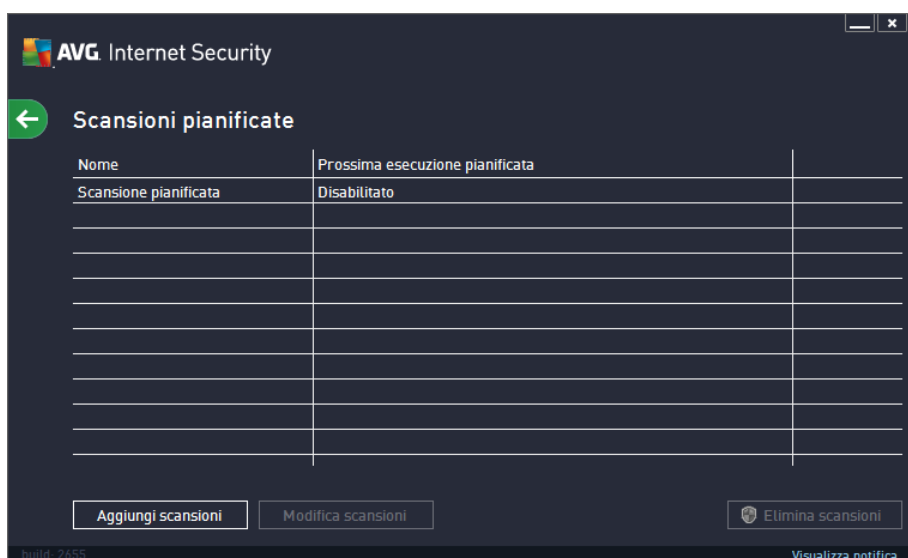
- /SCAN		Scansione file o cartelle /SCAN=percorso;percorso *(ad esempio /SCAN=C:\;D:\)*
- /COMP		Scansione intero computer
- /HEUR		Utilizza analisi euristica
- /EXCLUDE		Escludi percorso o file dalla scansione
- /@		File di comando /nome file/
- /EXT		Esegui scansione su queste estensioni /ad esempio EXT=EXE,DLL/
- /NOEXT		Non eseguire scansione su queste estensioni /ad esempio NOEXT=JPG/
- /ARC		Esegui scansione su archivi

- /CLEAN Pulisci automaticamente
- /TRASH Sposta file infetti in Quarantena virus
- /QT Controllo rapido
- /LOG Genera file risultati scansione
- /MACROW Segnala macro
- /PWDW Segnala file protetti da password
- /ARCBOMBSW Segnala archive bomb*(archivi compressi più volte)*
- /IGNLOCKED Ignora file bloccati
- /REPORT Rapporto sul file /nome file/
- /REPAPPEND Allega al file rapporto
- /REPOK Segnala file non infetti come OK
- /NOBREAK Non consentire interruzione CTRL-BREAK
- /BOOT Abilita controllo MBR/BOOT
- /PROC Scansione dei processi attivi
- /PUP Segnala programmi potenzialmente indesiderati
- /PUPEXT Segnala set potenziati di programmi potenzialmente indesiderati
- /REG Scansione Registro di sistema
- /COO Esegui scansione dei cookie
- /? Visualizza la Guida sull'argomento
- /HELP Visualizza la Guida sull'argomento
- /PRIORITY Imposta priorità scansione /bassa, automatica, alta/ *(vedere Impostazioni avanzate / Scansioni)*
- /SHUTDOWN Arresta computer al completamento della scansione
- /FORCESHUTDOWN Forza arresto del computer al completamento della scansione
- /ADS Esegui scansione flussi di dati alternativi *(solo NTFS)*
- /HIDDEN Segnala i file con estensione nascosta
- /INFECTABLEONLY Scansione dei soli file con estensioni infettabili

- /THOROUGHSCAN Attiva scansione completa
- /CLOUDCHECK Ricerca di falsi positivi
- /ARCBOMBSW Segnala file di archivio ricompressi

11.4. Pianificazione di scansioni

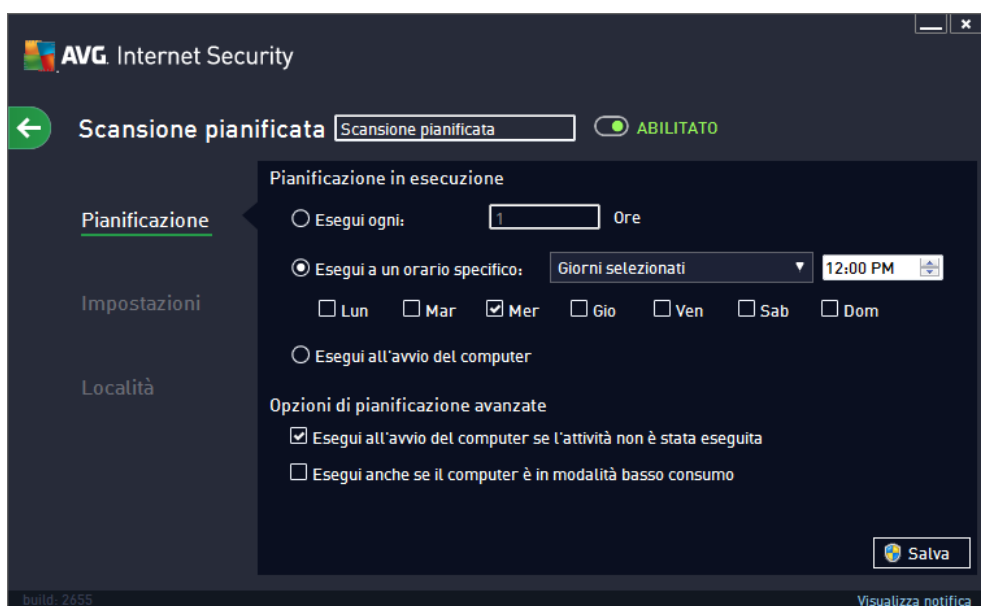
AVG Internet Security 2013 consente di eseguire scansioni su richiesta *(ad esempio quando si sospetta che un'infezione sia stata trasferita nel computer)* oppure in base a una pianificazione. Si consiglia di eseguire le scansioni in base a una pianificazione: in questo modo ci si assicura che il computer sia protetto da possibili infezioni e non è necessario preoccuparsi dell'avvio della scansione. Scansione intero computer deve essere avviata regolarmente, almeno una volta alla settimana. Tuttavia, se possibile, avviare la scansione dell'intero computer ogni giorno, come impostato nella configurazione predefinita della pianificazione della scansione. Se il computer è sempre acceso, è possibile pianificare le scansioni fuori dagli orari di lavoro. Se il computer rimane a volte spento, è possibile pianificare l'esecuzione delle scansioni all'avvio del computer, nel caso in cui l'attività non sia stata eseguita.

La pianificazione di scansione può essere creata / modificata nella finestra di dialogo ***Scansioni pianificate*** accessibile tramite il pulsante ***Gestione scansioni pianificate*** nella finestra di dialogo Opzioni di scansione. Nella nuova finestra di dialogo ***Scansione pianificata*** è possibile visualizzare una panoramica completa di tutte le scansioni pianificate al momento:

Prima di definire delle scansioni personalizzate, nell'elenco sarà possibile visualizzare solo una scansione pianificata predefinita dal fornitore del software. Per impostazione predefinita, la scansione è disattivata. Per attivarla, fare clic con il pulsante destro del mouse sull'opzione ***Abilita attività*** dal menu di scelta rapida. Dopo aver abilitato la scansione pianificata, è possibile modificare la relativa configurazione tramite il pulsante ***Modifica pianificazione scansione***. Inoltre, è possibile fare clic sul pulsante ***Aggiungi scansione pianificata*** per creare una nuova pianificazione di scansione personalizzata. È possibile modificare i parametri della scansione pianificata (*o configurare una nuova pianificazione*) in tre schede:

- Pianificazione

- Impostazioni
- Posizione

In ogni scheda è possibile impostare il pulsante "semaforo" per disattivare temporaneamente il controllo pianificato e riattivarlo secondo le necessità:

11.4.1. Pianificazione

Nella parte superiore della scheda ***Pianificazione*** è disponibile il campo di testo in cui specificare il nome della pianificazione di scansione che si sta definendo attualmente. Denominare le scansioni assegnando sempre nomi brevi, descrittivi e appropriati per poterle riconoscere più facilmente in futuro. Ad esempio, non è appropriato denominare una scansione "Nuova scansione" o "Scansione personale" poiché questi nomi non fanno riferimento agli elementi sottoposti a scansione. Tuttavia, un esempio di un buon nome descrittivo potrebbe essere "Scansione aree di sistema" e così via.

In questa finestra di dialogo è possibile definire ulteriormente i seguenti parametri della scansione:

- ***Pianificazione esecuzione***: consente di specificare gli intervalli di tempo per l'avvio della nuova scansione pianificata. È possibile definire l'ora tramite l'avvio ripetuto della scansione dopo un certo periodo di tempo *(Esegui ogni...)* oppure specificando data e ora esatte *(Esegui a determinati intervalli di tempo...)*) o specificando un evento a cui dovrà essere associato l'avvio della scansione *(Esegui all'avvio del computer)*.

- ***Opzioni di pianificazione avanzate***: questa sezione consente di definire le circostanze in cui deve essere avviata o non avviata la scansione se il computer si trova in modalità basso consumo oppure se è completamente spento. Quando la scansione pianificata viene avviata in corrispondenza dell'ora specificata, l'utente ne viene informato tramite una finestra popup visualizzata sopra l'icona della barra delle applicazioni di AVG. Viene quindi visualizzata una nuova icona della barra delle applicazioni di AVG (completamente colorata e con una luce lampeggiante) per comunicare che è in corso una scansione pianificata. Fare clic con il pulsante destro del mouse sull'icona AVG della scansione in esecuzione per aprire un menu di scelta rapida in cui è possibile decidere se sospendere o arrestare la scansione in

esecuzione, nonché modificarne la priorità.

Controlli nella finestra di dialogo

- ***Salva***: consente di salvare tutte le modifiche eseguite su questa scheda o su un'altra scheda della finestra di dialogo e di tornare alla panoramica delle scansioni pianificate. Pertanto, se si desidera configurare i parametri di controllo di tutte le schede, selezionare il pulsante per salvarli solo dopo aver specificato tutti i requisiti desiderati.

- : usare la freccia verde nella parte superiore sinistra della finestra di dialogo per tornare alla panoramica delle scansioni pianificate.

11.4.2. Impostazioni

Nella parte superiore della scheda ***Impostazioni*** è possibile trovare il campo di testo in cui specificare il nome della pianificazione di scansione che si sta definendo attualmente. Denominare le scansioni assegnando sempre nomi brevi, descrittivi e appropriati per poterle riconoscere più facilmente in futuro. Ad esempio, non è appropriato denominare una scansione "Nuova scansione" o "Scansione personale" poiché questi nomi non fanno riferimento agli elementi sottoposti a scansione. Tuttavia, un esempio di un buon nome descrittivo potrebbe essere "Scansione aree di sistema" e così via.

Nella scheda ***Impostazioni***è contenuto un elenco di parametri di scansione che possono essere attivati/disattivati facoltativamente. ***A meno che ci sia una ragione valida per modificare le impostazioni, si consiglia di mantenere la configurazione predefinita***:

- ***Correggi/Rimuovi infezioni da virus senza richiedere conferma*** *(attivata per impostazione predefinita):* se viene identificato un virus durante la scansione, può essere

corretto automaticamente se è disponibile una soluzione. Se il file infetto non può essere corretto automaticamente, l'oggetto infetto verrà spostato in Quarantena virus.

- ***Segnala programmi potenzialmente indesiderati e minacce spyware*** *(attivata per impostazione predefinita):* selezionare questa casella di controllo per attivare la scansione per ricercare spyware e virus. Gli spyware rappresentano una categoria di malware anomala: anche se solitamente costituiscono un rischio per la sicurezza, alcuni di questi programmi possono essere installati intenzionalmente. Si consiglia di mantenere questa funzionalità attivata in quanto consente di aumentare la protezione del computer.

- ***Segnala set potenziati di programmi potenzialmente indesiderati*** (*disattivata per impostazione predefinita*): selezionare questa casella di controllo per rilevare pacchetti estesi di spyware, ovvero programmi perfettamente normali e innocui al momento dell'acquisto diretto presso il produttore, ma utilizzabili a scopi dannosi successivamente. Si tratta di una precauzione aggiuntiva che aumenta ulteriormente la protezione del computer, ma che potrebbe bloccare programmi legittimi, pertanto l'opzione è disattivata per impostazione predefinita.

- ***Scansione dei cookie di rilevamento*** (*disattivata per impostazione predefinita*): questo parametro stabilisce che i cookie devono essere rilevati durante la scansione (*i cookie HTTP vengono utilizzati per autenticare, rilevare e mantenere informazioni specifiche sugli utenti, quali le preferenze dei siti o il contenuto dei carrelli elettronici*)

- ***Scansione all'interno degli archivi*** (*disattivata per impostazione predefinita*): questo parametro stabilisce che la scansione deve controllare tutti i file anche se inclusi all'interno di un tipo di archivio, quale ZIP, RAR e così via.

- ***Usa analisi euristiche*** (*attivata per impostazione predefinita*): l'analisi euristica (*emulazione dinamica delle istruzioni dell'oggetto sottoposto a scansione in un ambiente informatico virtuale*) sarà uno dei metodi utilizzati per il rilevamento di virus durante la scansione.

- ***Scansione ambiente di sistema*** (*attivata per impostazione predefinita*): la scansione verrà eseguita anche sulle aree di sistema del computer.

- ***Attiva scansione completa*** (*disattivata per impostazione predefinita):* in situazioni specifiche, *ad esempio se si sospetta che il computer sia stato infettato*, per maggiore sicurezza è possibile selezionare questa opzione per attivare gli algoritmi di scansione più completi che esamineranno anche le aree del computer che difficilmente vengono infettate. Tenere presente tuttavia che questo metodo è piuttosto dispendioso in termini di tempo.

- ***Ricerca di rootkit*** *(attivata per impostazione predefinita):* la scansione Anti-Rootkit cerca nel computer possibili rootkit, ovvero programmi e tecnologie che possono coprire l'attività dei malware nel computer. Se viene rilevato un rootkit, ciò non significa necessariamente che il computer sia infetto. In alcuni casi, specifici driver o sezioni di applicazioni regolari possono venire rilevati erroneamente come rootkit.

Impostazioni di scansione aggiuntive

Il collegamento consente di aprire una nuova finestra di dialogo ***Impostazioni di scansione aggiuntive*** in cui è possibile specificare i seguenti parametri:

- ***Opzioni arresto computer***: consente di decidere se il computer deve essere arrestato automaticamente al termine del processo di scansione. Dopo aver confermato questa opzione (*Arresta computer al completamento della scansione*), viene attivata una nuova opzione che consente l'arresto del computer anche se è correntemente bloccato *(Forza arresto se il computer è bloccato)*.

- ***Tipi di file per la scansione***: specificare se si desidera sottoporre a scansione:

  - ***Tutti i tipi di file*** con l'opzione per definire le eccezioni fornendo un elenco di estensioni di file separate da virgola da non sottoporre a scansione;

  - ***Tipi di file selezionati***: è possibile specificare che si desidera sottoporre a scansione solo file potenzialmente infettabili *(i file che non possono essere infettati non verranno sottoposti a scansione, ad esempio alcuni file di testo normale o altri file non eseguibili)*, inclusi i file multimediali *(file video e audio. Se non si seleziona questa casella, il tempo di scansione risulterà ulteriormente ridotto, poiché questi file sono spesso di grandi dimensioni e non facilmente infettabili da un virus)*. Anche in questo caso, è possibile specificare tramite le estensioni quali file devono essere sempre sottoposti a scansione.

  - Facoltativamente, è possibile effettuare la ***Scansione dei file senza estensioni***: questa opzione è attivata per impostazione predefinita e si consiglia di non modificarla a meno che non siano presenti motivi validi per farlo. I file senza estensione sono piuttosto sospetti e devono essere sempre sottoposti a scansione.

Regola la velocità di completamento della scansione

All'interno di questa sezione è inoltre possibile specificare la velocità di scansione desiderata in base all'utilizzo delle risorse di sistema. Per impostazione predefinita, questa opzione è impostata sul livello *Sensibile all'utente* per l'utilizzo automatico delle risorse. Se si desidera aumentare la velocità della scansione, il tempo impiegato sarà inferiore ma l'utilizzo delle risorse di sistema

aumenterà notevolmente durante l'esecuzione e rallenterà le altre attività svolte sul PC (*questa opzione può essere utilizzata quando il computer è acceso ma non è utilizzato*). Tuttavia, è possibile diminuire l'utilizzo delle risorse di sistema aumentando la durata della scansione.

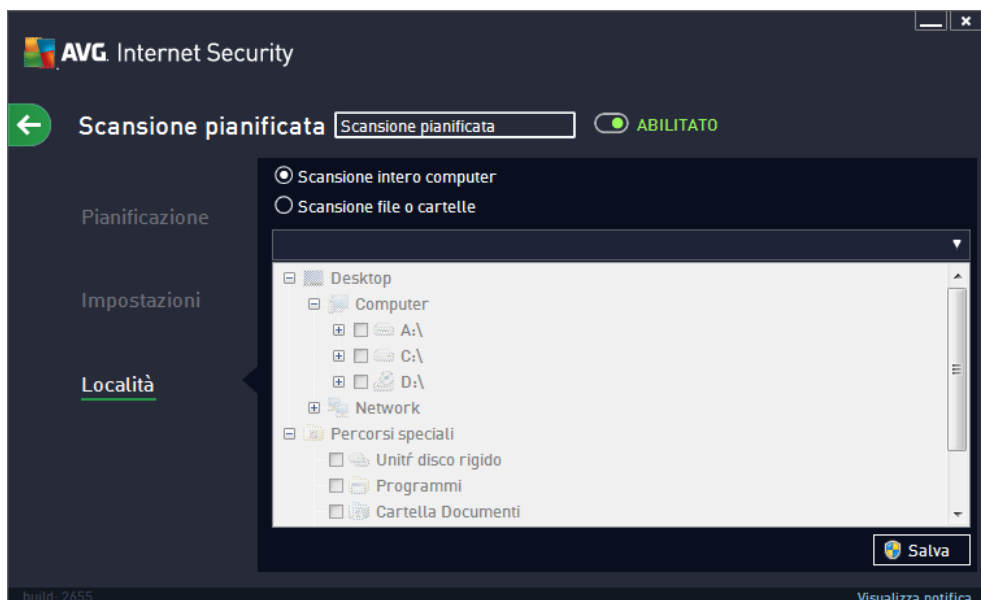
Imposta rapporti di scansione aggiuntivi

Fare clic sul collegamento ***Imposta rapporti di scansione aggiuntivi...*** per aprire una finestra di dialogo autonoma denominata ***Rapporti di scansione*** in cui è possibile selezionare diversi elementi per definire i tipi di rilevamenti da segnalare:

Controlli nella finestra di dialogo

- ***Salva***: consente di salvare tutte le modifiche eseguite su questa scheda o su un'altra scheda della finestra di dialogo e di tornare alla panoramica delle scansioni pianificate. Pertanto, se si desidera configurare i parametri di controllo di tutte le schede, selezionare il pulsante per salvarli solo dopo aver specificato tutti i requisiti desiderati.

- : usare la freccia verde nella parte superiore sinistra della finestra di dialogo per tornare alla panoramica delle scansioni pianificate.

11.4.3. Località

Nella scheda ***Posizione*** è possibile definire se si desidera pianificare la scansione dell'intero computer o la scansione di file o cartelle. Se si seleziona la scansione di cartelle o file, nella parte inferiore di questa finestra di dialogo viene attivata la struttura visualizzata che consente di specificare le cartelle da sottoporre a scansione (*espandere le voci facendo clic sul nodo "+" finché non viene individuata la cartella da sottoporre a scansione*). È possibile selezionare più cartelle facendo clic sulle rispettive caselle. Le cartelle selezionate verranno visualizzate nel campo di testo nella parte superiore della finestra di dialogo e nel menu a discesa verrà mantenuta la cronologia delle scansioni selezionate per riferimento futuro. In alternativa, è possibile immettere manualmente il percorso completo della cartella desiderata (*se si immettono più percorsi, è necessario separarli con un punto e virgola senza ulteriori spazi*).

All'interno della struttura è inoltre possibile visualizzare un ramo denominato ***Percorsi speciali***. Di seguito è disponibile un elenco delle posizioni che verranno sottoposte a scansione se verrà selezionata la relativa casella di controllo:

- ***Dischi rigidi locali***: tutti i dischi rigidi del computer
- ***Programmi***
  - o C:\Programmi\
  - o *nella versione a 64 bit* C:\Programmi (x86)
- ***Cartella Documenti***
  - o *per Windows XP:* C:\Documents and Settings\utente predefinito\Documenti\
  - o *per Windows Vista/7*: C:\Users\utente\Documenti\
- ***Documenti condivisi***

- o *per Windows XP*: C:\Documents and Settings\All Users\Documenti condivisi\
- o *per Windows Vista/7*: C:\Users\Public\Documenti condivisi\

- ***Cartella Windows***: C:\Windows\
- ***Altro***
  - o *Unità di sistema*: disco rigido su cui è installato il sistema operativo (solitamente C:)
  - o *Cartella di sistema*: C:\Windows\System32\
  - o *Cartella file temporanei*: C:\Documents and Settings\utente\Local\ (*Windows XP*) oppure C:\Users\utente\AppData\Local\Temp\ (*Windows Vista/7*)
  - o *File temporanei di Internet*: C:\Documents and Settings\utente\Local Settings\Temporary Internet Files\ (*Windows XP*); oppure C:\Users\utente\AppData\Local\Microsoft\Windows\Temporary Internet Files (*Windows Vista/7*)

Controlli nella finestra di dialogo

- ***Salva***: consente di salvare tutte le modifiche eseguite su questa scheda o su un'altra scheda della finestra di dialogo e di tornare alla panoramica delle scansioni pianificate. Pertanto, se si desidera configurare i parametri di controllo di tutte le schede, selezionare il pulsante per salvarli solo dopo aver specificato tutti i requisiti desiderati.
- : usare la freccia verde nella parte superiore sinistra della finestra di dialogo per tornare alla panoramica delle scansioni pianificate.

11.5. Risultati scansione

Nella finestra di dialogo ***Panoramica risultati di scansione*** è contenuto l'elenco dei risultati di tutte le scansioni eseguite in precedenza. Il grafico fornisce le seguenti informazioni su ciascun risultato della scansione:

- ***Icona***: nella prima colonna è visualizzata un'icona informativa che descrive lo stato della scansione:
  - Nessuna infezione rilevata, scansione completata
  - Nessuna infezione rilevata, scansione interrotta prima del completamento
  - Infezioni rilevate e non corrette, scansione completata
  - Infezioni rilevate e non corrette, scansione interrotta prima del completamento
  - Infezioni rilevate e corrette o rimosse, scansione completata
  - Infezioni rilevate e corrette o rimosse, scansione interrotta prima del completamento
- ***Nome***: in questa colonna viene visualizzato il nome della rispettiva scansione. Si tratta di una delle due scansioni predefinite oppure della scansione pianificata dall'utente.
- ***Ora di inizio***: indica la data e l'ora esatte di avvio della scansione.
- ***Ora di fine***: indica la data e l'ora esatte in cui la scansione è stata completata, sospesa o interrotta.
- ***Oggetti controllati***: indica il numero totale di tutti gli oggetti sottoposti a scansioni.
- ***Infezioni***: indica il numero di infezioni rilevate totali/rimosse.
- ***Alto / Medio / Basso***: le seguenti colonne indicano il numero di infezioni rilevate con livello di gravità alto, medio o basso rispettivamente.
- ***Rootkit***: indica il numero totale di rootkit rilevati durante la scansione.

Comandi della finestra di dialogo

Visualizza dettagli: fare clic sul pulsante per visualizzare informazioni dettagliate su una scansione selezionata *(evidenziata nel grafico sopra)*.

Elimina risultati: fare clic sul pulsante per rimuovere un risultato della scansione selezionato nel grafico.

: usare la freccia verde nella parte superiore sinistra della finestra di dialogo per tornare all' interfaccia utente principale con la panoramica dei componenti.

11.6. Dettagli di Risultati scansione

Per aprire una panoramica delle informazioni dettagliate su un risultato scansione selezionato, fare clic sul pulsante ***Visualizza dettagli*** disponibile nella finestra di dialogo Panoramica risultati di scansione. Si verrà reindirizzati alla stessa interfaccia che descrive dettagliatamente le informazioni sui rispettivi risultati della scansione. Le informazioni sono divise in tre schede:

- ***Riepilogo***: questa scheda fornisce informazioni di base sulla scansione, se è stata completata, se sono state rilevate minacce e l'operazione che è stata eseguita su di esse.

- ***Dettagli***: in questa scheda vengono visualizzate tutte le informazioni sulla scansione, inclusi i dettagli relativi a eventuali minacce rilevate. Esporta panoramica nel file consente di salvarla come file .csv.

- ***Rilevamenti***: questa scheda viene visualizzata solo se sono state rilevate minacce durante la scansione e fornisce informazioni dettagliate sulle minacce.

  Livello di gravità basso: informazioni o avvisi, non minacce effettive. In genere, documenti che contengono macro, documenti o archivi protetti da password, file bloccati e così via.

  Livello di gravità medio: in genere PUP *(programmi potenzialmente indesiderati, come adware)* o cookie di rilevamento

  Livello di gravità alto: minacce gravi come virus, trojan, exploit e così via. Anche oggetti individuati dal metodo di rilevamento dell'analisi euristica, ovvero minacce non ancora descritte nel database dei virus.

12. Quarantena virus

Quarantena virus è un ambiente protetto per la gestione degli oggetti sospetti o infetti rilevati durante i controlli AVG. Se durante la scansione viene rilevato un oggetto infetto e AVG non è in grado di ripararlo automaticamente, viene richiesto quale operazione eseguire sull'oggetto sospetto. La soluzione consigliata è spostare l'oggetto in ***Quarantena virus*** per un'ulteriore elaborazione. Lo scopo principale di ***Quarantena virus*** è quello di conservare ciascun file eliminato per un periodo di tempo sufficiente ad accertare che il file non sia più necessario nella posizione originale. Se l'assenza del file dovesse causare problemi, è possibile inviare il file in questione per l'analisi o ripristinarlo nella posizione originale.

L'interfaccia di ***Quarantena virus*** viene aperta in una finestra separata e offre una panoramica delle informazioni relative agli oggetti infetti messi in quarantena:

- ***Gravità***: se è stato installato il componente Identity in **AVG Internet Security 2013**, questa sezione fornirà l'identificazione grafica della gravità del rilevamento in base a una scala a quattro livelli dal più sicuro ((*tre punti verdi)* al più pericoloso *(tre punti rossi)* e informazioni sul tipo di infezione (*in base al livello di infezione, tutti gli oggetti elencati possono essere decisamente o potenzialmente infetti*)
- ***Nome virus***: specifica il nome dell'infezione rilevata in base all'enciclopedia dei virus
- ***Percorso del file***: percorso completo della posizione originale del file infetto rilevato
- ***Data di archiviazione***: data e ora del rilevamento e dell'inserimento in Quarantena virus

Pulsanti di controllo

I seguenti pulsanti di controllo sono accessibili dall'interfaccia di ***Quarantena virus***:

- ***Ripristina***: consente di ripristinare il file infetto nella posizione originale sul disco
- ***Ripristina come***: sposta il file infetto nella cartella selezionata
- ***Dettagli***: per informazioni dettagliate sulla minaccia specifica spostata in ***Quarantena virus*** evidenziare l'elemento selezionato nell'elenco e fare clic sul pulsante ***Dettagli*** per aprire una nuova finestra di dialogo con la descrizione della minaccia rilevata.
- ***Elimina***: consente di rimuovere definitivamente il file infetto da ***Quarantena virus***
- ***Svuota Quarantena***: elimina completamente tutto il contenuto di ***Quarantena Virus***. I file rimossi da ***Quarantena virus*** vengono eliminati in modo definitivo dal disco (*non vengono spostati nel Cestino*).

13. Cronologia

La sezione ***Cronologia*** include informazioni su tutti gli eventi precedenti *(ad esempio aggiornamenti, scansioni, rilevamenti e così via)* e i rapporti relativi a tali eventi. Questa sezione è accessibile dall' interfaccia utente principale tramite la voce ***Opzioni / Cronologia***. Inoltre, la cronologia di tutti gli eventi registrati è suddivisa nelle seguenti parti:

- Risultati scansione
- Rilevamento Resident Shield
- Rilevamento Protezione e-mail
- Rilevamenti di Online Shield
- Log cronologia eventi
- Log Firewall

13.1. Risultati scansione

La finestra di dialogo ***Panoramica risultati di scansione*** è accessibile tramite la voce ***Opzioni / Cronologia / Risultati scansione*** nel menu di spostamento superiore della finestra principale di **AVG Internet Security 2013**. Nella finestra di dialogo è contenuto l'elenco di tutte le scansioni avviate in precedenza e le informazioni sui relativi risultati:

- ***Nome***: nome della scansione; può essere il nome di una delle scansioni predefinite o il nome assegnato alla propria scansione pianificata. Ciascun nome include un'icona che indica i risultati della scansione:

  – il colore verde indica che non è stata rilevata alcuna infezione durante la

scansione

– il colore blu indica che è stata rilevata un'infezione durante la scansione ma l'oggetto infetto è stato rimosso automaticamente

– il colore rosso indica che è stata rilevata un'infezione durante la scansione ma non è stato possibile rimuoverla.

Ciascuna icona può essere intera o suddivisa in due parti: l'icona intera indica una scansione completata correttamente, l'icona suddivisa in due indica una scansione annullata o interrotta.

Nota*: per informazioni dettagliate su ciascuna icona vedere la finestra di dialogo Risultati scansione accessibile tramite il pulsante Visualizza dettagli (nella parte inferiore della finestra di dialogo).*

- ***Ora di inizio***: data e ora di avvio della scansione
- ***Ora di fine***: data e ora del completamento della scansione
- ***Oggetti controllati***: numero di oggetti controllati durante la scansione
- ***Infezioni***: numero delle infezioni da virus rilevate / rimosse
- ***Alto / Medio*** / ***Basso***: queste colonne indicano il numero di infezioni totali/rimosse con livello di gravità alto, medio o basso rispettivamente
- ***Informazioni***: informazioni relative all'andamento e al risultato della scansione *(in genere in relazione alla finalizzazione o all'interruzione)*
- ***Rootkit***: numero di rootkit

Pulsanti di controllo

I pulsanti di controllo per la finestra di dialogo ***Panoramica risultati di scansione*** sono i seguenti:

- ***Visualizza dettagli***: selezionare questa opzione per accedere alla finestra di dialogo Risultati scansione e visualizzare dati dettagliati relativi alla scansione selezionata
- ***Elimina risultato***: selezionare questa opzione per rimuovere la voce selezionata dalla panoramica dei risultati di scansione
- : per tornare alla finestra di dialogo principale di AVG *predefinita (panoramica dei componenti),* utilizzare la freccia nell'angolo superiore sinistro di questa finestra di dialogo

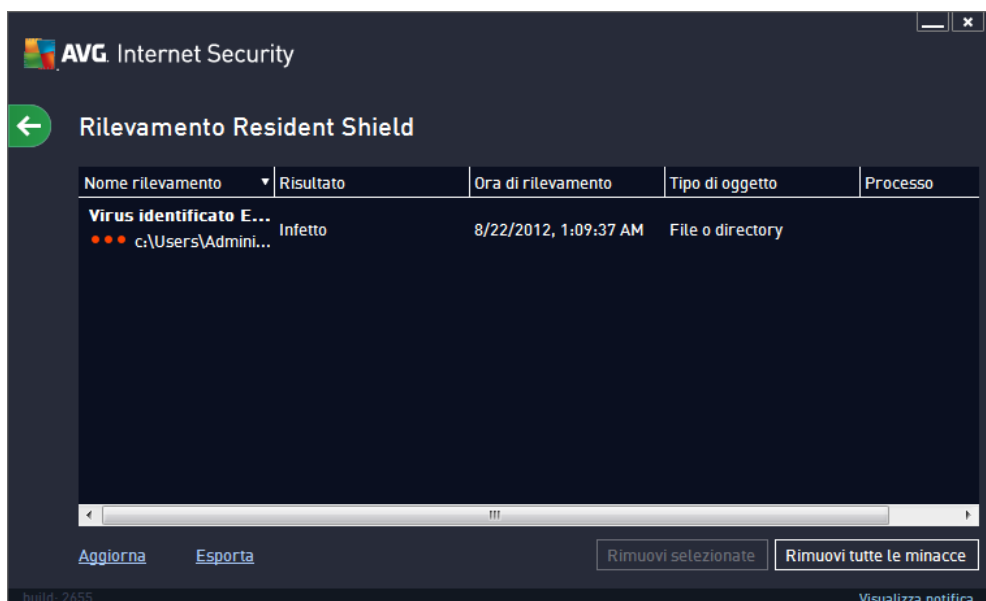
13.2. Rilevamento Resident Shield

Il servizio ***Resident Shield*** fa parte del componente ***Computer*** ed esegue la scansione dei file mentre vengono copiati, aperti o salvati. Quando viene rilevato un virus o altra minaccia, l'utente viene avvisato immediatamente tramite la successiva finestra di dialogo:

In questa finestra di dialogo di avviso sono disponibili delle informazioni sull'oggetto rilevato e giudicato infetto (*Nome*) e alcuni fatti descrittivi sull'infezione riconosciuta (*Descrizione*). Selezionando il collegamento Mostra dettagli si verrà reindirizzati all'enciclopedia dei virus in rete in cui è possibile trovare informazioni dettagliate sull'infezione rilevata, se note. Nella finestra di dialogo verrà inoltre visualizzata una panoramica delle soluzioni disponibili per gestire la minaccia rilevata. Una delle alternative verrà contrassegnata come consigliata: ***Proteggimi (scelta consigliata). Se possibile, si consiglia di attenersi sempre a questa opzione.***

Nota: *potrebbe accadere che le dimensioni dell'oggetto rilevato superino il limite di spazio libero in Quarantena virus. In tal caso, verrà visualizzato un avviso relativo al problema quando si tenterà di spostare l'oggetto infetto in Quarantena virus. Tuttavia, le dimensioni di Quarantena virus possono essere modificate. Tali dimensioni vengono definite come percentuale regolabile delle dimensioni effettive del disco rigido. Per aumentare le dimensioni di Quarantena virus, nella finestra di dialogo Quarantena virus, accessibile tramite Impostazioni AVG avanzate, è disponibile l'opzione Limite dimensione per Quarantena virus.*

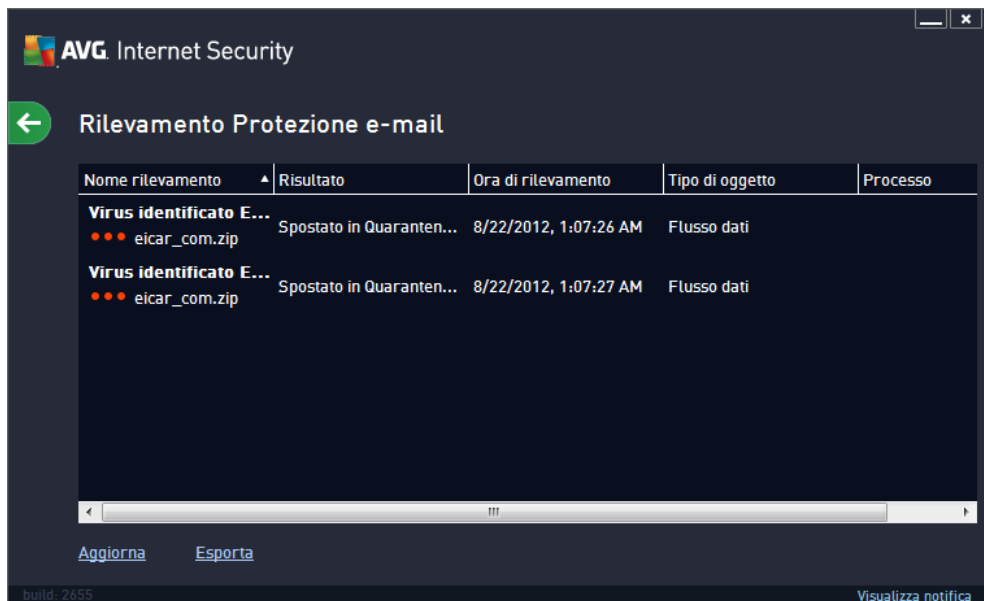
Nella parte inferiore della finestra di dialogo è possibile trovare il collegamento ***Mostra dettagli***. Fare clic sul pulsante per aprire una nuova finestra con informazioni dettagliate sul processo in esecuzione durante il rilevamento dell'infezione e i dati identificativi del processo.

Un elenco di tutti i rilevamenti di Resident Shield è disponibile per una panoramica all'interno della finestra di dialogo ***Rilevamento Resident Shield***. Questa finestra di dialogo è accessibile tramite la voce ***Opzioni / Cronologia / Rilevamento Resident Shield*** nel menu di spostamento superiore della finestra principale di **AVG Internet Security 2013**. Nella finestra di dialogo è disponibile una panoramica di oggetti rilevati da Resident Shield, classificati come pericolosi e corretti o spostati in Quarantena virus.

Per ogni oggetto rilevato vengono fornite le seguenti informazioni:

- ***Nome rilevamento***: descrizione (*possibilmente anche il nome*) dell'oggetto rilevato e la relativa posizione
- ***Risultato***: azione eseguita sull'oggetto rilevato
- ***Ora di rilevamento***: data e ora in cui la minaccia è stata rilevata e bloccata
- ***Tipo di oggetto***: tipo di oggetto rilevato
- ***Processo***: operazione eseguita per richiamare e rilevare l'oggetto potenzialmente pericoloso

Pulsanti di controllo

- ***Aggiorna***: consente di aggiornare l'elenco dei rilevamenti effettuati da ***Online Shield***
- ***Esporta***: consente di esportare l'intero elenco di oggetti rilevati in un file
- ***Rimuovi voci selezionate***: nell'elenco è possibile evidenziare i record selezionati e utilizzare questo pulsante per eliminare solo tali elementi
- ***Rimuovi tutte le minacce***: fare clic su questo pulsante per eliminare tutti i record elencati in questa finestra di dialogo
- : per tornare alla finestra di dialogo principale di AVG *predefinita (panoramica dei componenti),* utilizzare la freccia nell'angolo superiore sinistro di questa finestra di dialogo

13.3. Rilevamento Protezione e-mail

La finestra di dialogo ***Rilevamento Scansione E-mail*** è accessibile tramite la voce ***Opzioni / Cronologia / Rilevamento Scansione E-mail*** nel menu di spostamento superiore della finestra principale di **AVG Internet Security 2013**. La finestra di dialogo fornisce un elenco di tutti i rilevamenti effettuati dal componente Protezione e-mail . Per ogni oggetto rilevato vengono fornite le seguenti informazioni:

- ***Infezione***: descrizione (eventualmente anche il nome) dell'oggetto rilevato
- ***Oggetto***: posizione dell'oggetto
- ***Risultato***: azione eseguita sull'oggetto rilevato
- ***Ora di rilevamento***: data e ora in cui l'oggetto sospetto è stato rilevato
- ***Tipo di oggetto***: tipo di oggetto rilevato

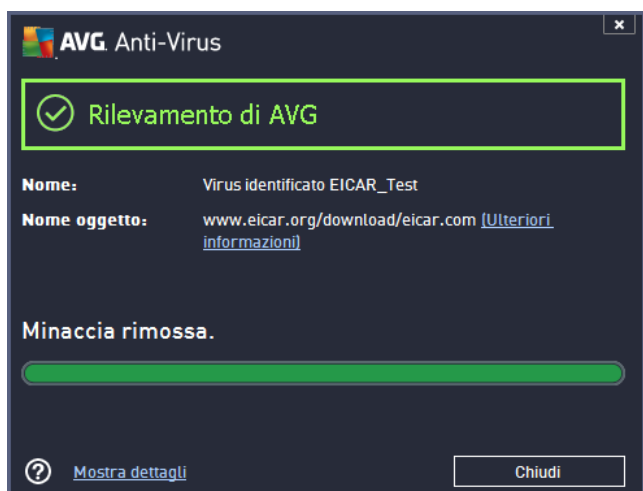
Nella parte inferiore della finestra di dialogo, sotto l'elenco, sono disponibili informazioni sul numero totale degli oggetti rilevati elencati sopra. È inoltre possibile esportare l'intero elenco di oggetti rilevati in un file (***Esporta elenco in file***) ed eliminare tutte le voci relative agli oggetti rilevati (***Svuota elenco***).

Pulsanti di controllo

I pulsanti di controllo disponibili nell'interfaccia di ***Rilevamento Scansione E-mail*** sono i seguenti:

- ***Aggiorna elenco***: aggiorna l'elenco delle minacce rilevate.
- : per tornare alla finestra di dialogo principale di AVG *predefinita (panoramica dei componenti),* utilizzare la freccia nell'angolo superiore sinistro di questa finestra di dialogo

13.4. Rilevamenti di Online Shield

Online Shield esegue la scansione del contenuto delle pagine Web visitate e dei possibili file in esse contenuti prima che queste vengano visualizzate nel browser Web o scaricate nel computer. Se viene rilevata una minaccia, l'utente verrà avvisato immediatamente tramite la seguente finestra di dialogo:

In questa finestra di dialogo di avviso sono disponibili delle informazioni sull'oggetto rilevato e giudicato infetto (*Nome*) e alcuni fatti descrittivi sull'infezione riconosciuta (*Descrizione*). Selezionando il collegamento Mostra dettagli si verrà reindirizzati all'enciclopedia dei virus in rete in cui è possibile trovare informazioni dettagliate sull'infezione rilevata, se note. La finestra di dialogo fornisce i seguenti elementi di controllo:

- ***Mostra dettagli***: fare clic sul collegamento per aprire una nuova finestra popup con informazioni sul processo in esecuzione durante il rilevamento dell'infezione e i dati identificativi del processo.
- ***Chiudi***: fare clic sul pulsante per chiudere la finestra di dialogo di avviso.

La pagina Web sospetta non verrà aperta e il rilevamento della minaccia verrà registrato nell'elenco ***Rilevamenti di Online Shield***. Questa panoramica di minacce rilevate è accessibile tramite la voce ***Opzioni / Cronologia / Rilevamenti di Online Shield*** nel menu di spostamento superiore della finestra principale di **AVG Internet Security 2013**.

Per ogni oggetto rilevato vengono fornite le seguenti informazioni:

- ***Nome rilevamento***: descrizione (*possibilmente anche il nome*) dell'oggetto rilevato e la relativa origine (*pagina Web*)
- ***Risultato***: azione eseguita sull'oggetto rilevato
- ***Ora di rilevamento***: data e ora in cui la minaccia è stata rilevata e bloccata
- ***Tipo di oggetto***: tipo di oggetto rilevato
- ***Processo***: operazione eseguita per richiamare e rilevare l'oggetto potenzialmente pericoloso

Pulsanti di controllo

- ***Aggiorna***: consente di aggiornare l'elenco dei rilevamenti effettuati da ***Online Shield***
- ***Esporta***: consente di esportare l'intero elenco di oggetti rilevati in un file
- : per tornare alla finestra di dialogo principale di AVG *predefinita (panoramica dei componenti),* utilizzare la freccia nell'angolo superiore sinistro di questa finestra di dialogo

13.5. Log cronologia eventi

La finestra di dialogo ***Log cronologia eventi*** è accessibile tramite la voce di menu ***Opzioni / Cronologia / Log cronologia eventi*** nel menu di spostamento superiore della finestra principale di **AVG Internet Security 2013**. In questa finestra di dialogo è possibile trovare un riepilogo di importanti eventi che si sono verificati durante l'attività di **AVG Internet Security 2013**. La finestra di dialogo fornisce i record dei seguenti tipi di eventi: informazioni sugli aggiornamenti dell'applicazione AVG, informazioni sull'inizio, la fine o l'arresto della scansione (*inclusi i controlli eseguiti automaticamente*), informazioni sugli eventi connessi al rilevamento di un virus (*tramite la protezione permanente o la scansione*) inclusa la relativa posizione e altri eventi importanti.

Per ciascun evento vengono indicate le seguenti informazioni:

- ***Data e ora evento*** indica la data e l'ora esatte in cui si è verificato l'evento
- ***Utente*** indica il nome dell'utente connesso nel momento in cui si è verificato l'evento
- ***Origine*** fornisce informazioni sul componente di origine o altra parte del sistema AVG che ha attivato l'evento
- ***Descrizione evento*** presenta un breve riepilogo dell'evento che si è verificato

Pulsanti di controllo

- ***Aggiorna elenco***: fare clic su questo pulsante per aggiornare tutte le voci incluse nell'elenco degli eventi
- ***Chiudi***: fare clic sul pulsante per tornare alla finestra principale di **AVG Internet Security**

13.6. Firewall log

La finestra di dialogo ***Log*** consente di visualizzare l'elenco di tutte le azioni e gli eventi registrati di Firewall con una descrizione dettagliata dei parametri rilevanti mostrata in due schede:

- ***Log traffico***: questa scheda fornisce informazioni sull'attività di tutte le applicazioni che hanno tentato di connettersi alla rete. Per ognuna di queste, saranno incluse informazioni relative a ora dell'evento, nome dell'applicazione, rispettiva azione log, nome utente, PID, direzione del traffico, tipo di protocollo, numeri delle porte remote e locali e informazioni sull'indirizzo IP remoto e locale.

- ***Log database attendibile***: il *Database attendibile* è un database interno di AVG che raccoglie informazioni sulle applicazioni certificate e attendibili che saranno sempre autorizzate a comunicare in linea. La prima volta in cui una nuova applicazione tenta di connettersi alla rete (*ossia quando non è ancora stata specificata alcuna regola firewall per tale applicazione*), è necessario stabilire se la comunicazione di rete deve essere consentita per tale applicazione. Innanzitutto, AVG effettua una ricerca nel *Database attendibile*. Se l'applicazione è elencata, sarà automaticamente autorizzata ad accedere alla rete. Se nel database non sono presenti informazioni sull'applicazione, verrà richiesto in una nuova finestra di dialogo se si desidera autorizzare l'applicazione ad accedere alla rete.

Pulsanti di controllo

- ***Aggiorna elenco***: tutti i parametri registrati possono essere ordinati in base all'attributo selezionato: cronologicamente (*date*) o alfabeticamente (*altre colonne*). È sufficiente fare clic sull'intestazione di colonna pertinente. Utilizzare il pulsante ***Aggiorna elenco*** per aggiornare le informazioni visualizzate.

- ***Elimina log***: fare clic per eliminare tutte le voci presenti nel grafico.

14. Aggiornamenti di AVG

Nessun software di protezione è in grado di garantire una vera protezione dai vari tipi di minacce se non viene aggiornato con regolarità. Gli autori dei virus ricercano di continuo nuove imperfezioni da sfruttare sia nei sistemi operativi che nel software. Tutti i giorni si presentano nuovi virus, nuovi malware e nuovi attacchi di hacker. Per questa ragione, i fornitori di software rilasciano regolarmente aggiornamenti e patch di protezione per correggere eventuali difetti della protezione che vengono rilevati.

Considerando le nuove minacce informatiche emergenti e la velocità con cui si diffondono, è assolutamente fondamentale aggiornare **AVG Internet Security 2013** regolarmente. La soluzione migliore è attenersi alle impostazioni predefinite del programma in cui è stato configurato l'aggiornamento automatico. Tenere presente che, se il database dei virus di **AVG Internet Security 2013** non è aggiornato, il programma non sarà in grado di rilevare le minacce più recenti.

È fondamentale aggiornare AVG con regolarità. Gli aggiornamenti delle definizione dei virus principali dovrebbero essere eseguiti ogni giorno, se possibile. Gli aggiornamenti del programma meno urgenti possono essere eseguiti settimanalmente.

14.1. Avvio degli aggiornamenti

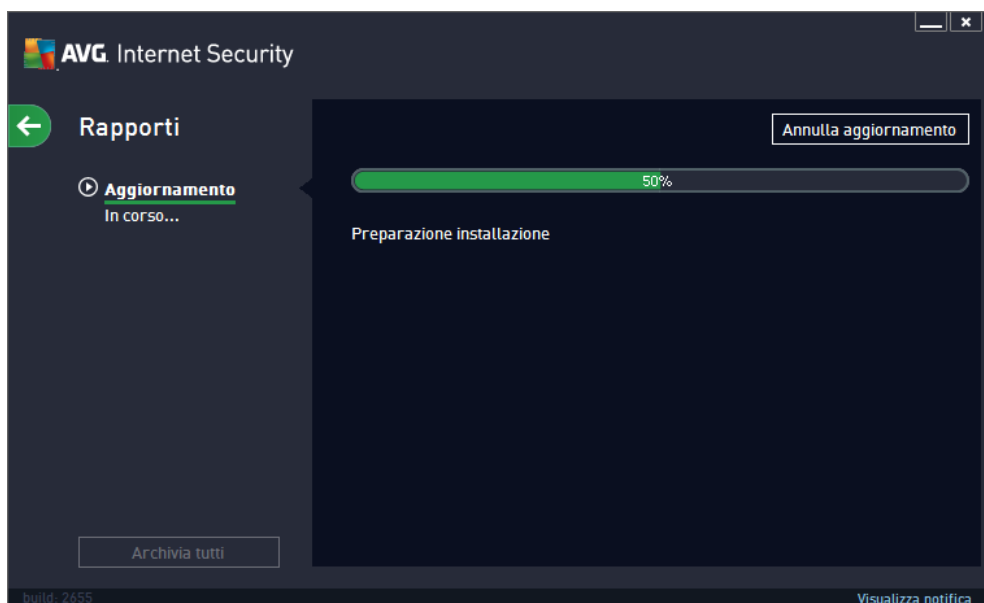
Per fornire la protezione massima, **AVG Internet Security 2013** per impostazione predefinita ricerca nuovi aggiornamenti del database dei virus ogni quattro ore. Poiché gli aggiornamenti AVG non vengono rilasciati in base a una pianificazione fissa, ma in base alla quantità e alla gravità di nuove minacce, questo check-up è molto importante per assicurare che il database dei virus di AVG sia sempre aggiornato.

Se si desiderasse ridurre il numero di aggiornamenti avviati, è possibile impostare parametri di avvio degli aggiornamenti personalizzati. Tuttavia, si consiglia di avviare l'aggiornamento almeno una volta al giorno. La configurazione può essere modificata nella sezione Impostazioni avanzate/ Pianificazioni, in particolare nelle seguenti finestre di dialogo:

- Pianificazione aggiornamento definizioni
- Pianificazione aggiornamento del programma
- Pianificazione aggiornamenti Anti-Spam

Per controllare la presenza di nuovi file di aggiornamento immediatamente, utilizzare il collegamento rapido Aggiorna adesso nell'interfaccia utente principale. Questo collegamento è sempre disponibile da qualsiasi finestra di dialogo dell'interfaccia utente.

14.2. Avanzamento dell'aggiornamento

Una volta avviato l'aggiornamento, AVG verificherà innanzitutto se sono presenti nuovi file di aggiornamento. In caso affermativo, **AVG Internet Security 2013** ne effettuerà il download e avvierà il processo di aggiornamento automaticamente. Durante il processo di aggiornamento si verrà reindirizzati all'interfaccia di ***Rapporti***, da cui è possibile visualizzare la rappresentazione grafica e la panoramica dei parametri statistici rilevanti dell'avanzamento del processo *(dimensione dei file di aggiornamento, dati ricevuti, velocità di download, tempo trascorso e così via)*:

14.3. Livelli di aggiornamento

AVG Internet Security 2013 offre due livelli di aggiornamento selezionabili:

- ***In Aggiornamento definizioni*** sono contenute le modifiche necessarie per una protezione anti-virus, anti-spam e anti-malware affidabile. In genere, non include eventuali modifiche del codice e consente di aggiornare solo il database delle definizioni. Questo aggiornamento deve essere applicato non appena si rende disponibile.

- ***In Aggiornamento programma*** sono presenti le modifiche, le correzioni e i miglioramenti del programma.

Nel corso della pianificazione di un aggiornamento, è possibile definire parametri specifici per entrambi i livelli di aggiornamento:

- Pianificazione aggiornamento definizioni

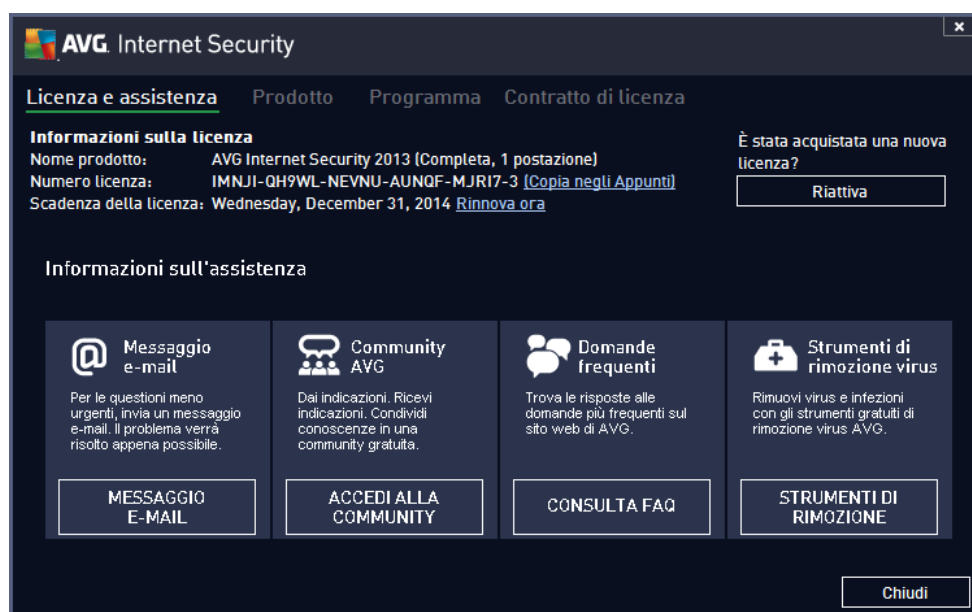
- Pianificazione aggiornamento del programma

Nota: *se gli orari di un aggiornamento del programma pianificato e di una scansione pianificata dovessero coincidere, il processo di aggiornamento acquista priorità e la scansione viene interrotta.*

15. Domande frequenti e assistenza tecnica

Se si verificano problemi di tipo commerciale o tecnico con l'applicazione **AVG Internet Security 2013** , sono disponibili diversi modi per richiedere assistenza. Effettuare la scelta tra le seguenti opzioni:

- ***Ottieni assistenza***: direttamente dall'applicazione AVG è possibile visualizzare una pagina dedicata dell'assistenza clienti sul sito Web di AVG (http://www.avg.com/). Selezionare la voce del menu principale ***Guida / Ottieni assistenza*** per essere reindirizzati a una pagina del sito Web di AVG con le opzioni di assistenza disponibili. Per procedere, seguire le istruzioni fornite nella pagina Web.

- ***Assistenza (collegamento nel menu principale)***: il menu dell'applicazione AVG (*nella parte superiore dell'interfaccia utente principale*) include il collegamento ***Assistenza*** che apre una nuova finestra di dialogo contenente tutti i tipi di informazioni necessarie per ricevere assistenza. La finestra di dialogo include dati di base sul programma AVG installato (*versione programma/database*), dettagli della licenza e un elenco di collegamenti rapidi per l'assistenza:

- ***Risoluzione dei problemi nella Guida***: una nuova sezione ***Risoluzione dei problemi*** è disponibile direttamente nel file della Guida incluso in **AVG Internet Security 2013** *(per aprire il file della Guida, premere il tasto F1 in qualsiasi finestra di dialogo nell'applicazione)*. Questa sezione fornisce un elenco delle situazioni che con maggiore frequenza spingono un utente a ricercare assistenza professionale per un problema tecnico. Selezionare la situazione che descrive meglio il problema corrente e fare clic sul collegamento per aprire le istruzioni dettagliate per la risoluzione del problema.

- ***Centro di assistenza del sito Web di AVG***: in alternativa, è possibile ricercare la soluzione al problema nel sito Web di AVG (http://www.avg.com/). Nella sezione ***Centro di assistenza*** è disponibile una panoramica strutturata di gruppi tematici che trattano problemi commerciali e tecnici.

- ***Domande frequenti***: sul sito Web di AVG (http://www.avg.com/) è inoltre disponibile

un'ampia sezione separata di domande frequenti. Questa sezione è accessibile tramite l'opzione di menu ***Centro di assistenza / Domande frequenti***. Anche in questo caso, tutte le domande sono suddivise chiaramente nelle categorie commerciale, tecnica e virus.

- ***Informazioni su virus e minacce***: una parte specifica del sito Web di AVG (http://www.avg.com/) è dedicata ai virus *(la pagina Web è accessibile dal menu principale tramite l'opzione Guida / Informazioni su virus e minacce)*. Nel menu, selezionare ***Centro di assistenza / Informazioni su virus e minacce*** per visualizzare una pagina che fornisce una panoramica strutturata di informazioni correlate alle minacce in linea. Sono inoltre disponibili istruzioni sulla rimozione di virus e spyware e consigli relativi alla protezione.

- ***Forum di discussione***: è inoltre possibile utilizzare il forum di discussione degli utenti AVG disponibile all'indirizzo http://forums.avg.com.